Marketplace Risk.

MASTERING MARKETPLACE RISK

Expert Advice from Industry Leaders

MASTERING MARKETPLACE RISK

Smart Advice from Founders, Operators & Experts Leading the Industry

This eBook features experts sharing their real-world experiences and tested strategies on marketplace risk topics ranging from digital identity, screening, trust & safety, payments & fraud prevention, data privacy, cybersecurity, regulatory & compliance, legal strategy, product & technology innovation - and everything in between.

About the Marketplace Risk Management Conference

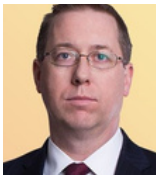
The Marketplace Risk Management Conference (MRMC) is the most comprehensive source for marketplaces and platforms to learn, network and share information about risk management, trust & safety, compliance and legal strategy necessary to launch, grow and exit successfully.

MRMC is essential for marketplaces and platforms of all stages. Whether you're an investor, founder, executive or operator, or a vendor or solution provider that they rely on, the MRMC agenda is packed with a diverse range of content to help you to avoid distraction so that you can launch, grow and exit successfully. This eBook features the best advice shared at the 2022 event. If you have any questions, please do not hesitate to reach out to us!

TABLE OF CONTENTS

Insight NO. 1:

Privacy Trends: CCPA, GDPR and Multi-State Enforcement Impacting Platforms



Chris Burris
Partner
King & Spalding LLP

Jason Priebe
Partner
Seyfarth Shaw

Anne Voigts
Partner
King & Spalding LLP

The principal cause for increased awareness of data protection and data security is the extreme risk involved. There's been an explosion of ransomware and hacking attacks, with twice the number of zero-day vulnerabilities year-over-year, with no sign of this trend slowing down. If there's a data breach and data is stolen or lost, organizations must understand their legal obligations. Any breach resulting in stolen or lost data can lead to increased scrutiny by regulators, class action lawsuits, or significant damage to the company's reputation. The targets of these attacks are wide-ranging, with attackers becoming increasingly sophisticated.

Our observations have revealed that service providers and organizations that handle data, including employee records, medical records, and payments, have taken a hit due to the increase in cyber attacks. These malicious activities have become more complex and have caused some companies to be completely paralyzed and unaware of vulnerabilities. This puts them at risk for non-compliance and can lead to serious legal problems.

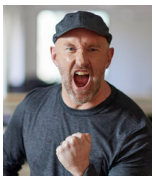
Since the California Consumer Privacy Act (CCPA) was enacted on January 1, 2020, over 250 lawsuits have been filed, largely due to data breaches. However, this is not the only cause of litigation. There have been allegations of misleading language and privacy policies that violate the CCPA's complex rules on handling customer data, obtaining user consent, and making mandatory notifications. Various other states have also passed laws, although none of them allow private rights of action. The plaintiffs and state attorney generals have shown creativity in the different approaches they've taken.

It isn't necessary to have a specific statute regarding privacy. Plaintiffs have been taking advantage of existing statutes like those for unfair competition and false advertisement to address the matter. An unexpected element is securities litigation. If the company is public or wants to go public, securities lawyers are now involved.

A major distinction between CCPA and other privacy laws is that California has adopted a definition of personal data that resembles the GDPR or the European model more closely. In the past, when dealing with privacy law, we focused on specific data categories and functions of the company, such as GLBA for banking, HIPAA for health care. Then there was the category of personal identifiable information (PII) and personal health information (PHI). Today, however, the European model has created a more general categorization of personal information and data.

Insight NO. 2:

Terms of Service: Your Marketplace's First Line of Defense (And What's on the Horizon)



Brian Powers
General Manager
Ironclad

You may not give much thought to your online terms of service agreement, but you should. Why is it so crucial? It's a binding contract between your company and your customers, and should be taken seriously. This type of agreement is mostly used in marketplace and e-commerce business models. Terms of service agreements aim to reduce risk for the business, like any other contract. It includes waivers, such as a disclaimer concerning goods and services offered, indemnity assurances, protection of the company's intellectual property, use of data, how refunds work, and more.

Within the body of law covering terms of service agreements, the focus is primarily on exemptions from class action lawsuits and binding arbitration. Businesses with millions of customers don't want to be sued by all of them at once, so they ensure customers waive their class action lawsuit rights and have them agree to arbitrate individually. This is not beneficial to customers, but advantageous for the business. Additionally, there are state-by-state auto-renew statutes that must be followed to properly collect consent and ensure terms are accurate. Invalid, unenforceable online legal terms render these protections meaningless, so it’s essential to get them right.

To be valid, a contract must be legally binding. It would be unwise to disregard this fact when drafting a contract intended to be signed through electronic means. People often make careless mistakes with terms of service agreements, thinking of them as insignificant. It’s important to remember that these are real contracts, and they must be treated as such. We’d never create a contract that’s unsigned or illegible, hard to find, or not saved in our records.

If someone agrees to the terms of service on a website, it's usually done in one of three ways. First, there's the clickwrap agreement, in which a person must check a box to confirm acceptance. This is an explicit act, which doesn’t require the person to read the terms, but provides assurance that they accept them. The second option is the browsewrap agreement. In this case, a link is placed in the footer, which states that the visitor agrees to the terms by browsing the website. This type of agreement isn't enforceable and should be avoided, as it doesn't require specific action.. The third type of agreements are sign-in wraps, which are a hybrid of creating an account and agreeing to terms in a single action. These agreements are not as good as clickwraps, but people see terms and take action, so they’re better than browsewraps. When it comes to litigation, our study revealed enforceability based on service agreement type, and the results were 75% enforceable for clickwrap, 64% for sign-in-wrap, and 0% for browsewrap agreements.

Insight NO. 3:

Government Relations & Public Policy: How to Engage in the Early Years

Heather Lewis
Director, Community
DISCO

Daniel Serota
Director of Public Affairs
Aon

The terms "government relations" and "government affairs" are interchangeable. They describe how organizations communicate with governments to educate lawmakers and other stakeholders about proposed laws, regulations, and the potential impact they may have on the organization and, in the case of marketplaces, users. It's also common to call it "public affairs," which focuses on how an organization communicates with legislators to showcase its brand and strengthen its reputation.

There are three types of government affairs: local, state and federal. Local involves working with city councils and chambers of commerce through local trade associations. At the state level, you're working with state government agencies, senators and house representatives. In some states, there is an insurance commissioner who regulates public insurance policies for the industry. At the federal level, the White House, Congress, government agencies, and trade associations of US chambers, business round tables, and digital chambers are all members with whom government affairs teams deal daily. On a global level, most other countries have similar government equivalents at each of these levels.

There are a few key issues faced by marketplaces, including worker classification (CA AB5, Prop 22), zoning and taxation. Insurance is also an enormous concern. Whenever you're dealing with an innovative space, education is a must, as many politicians may not be aware of it. Proactive engagement allows you to introduce yourself and share your company's narrative before government stakeholders learn about you from other parties, so that you can control the conversation. It allows you to develop positive relationships before you need them. At the same time, it puts you on their radar and opens the door for your organization to be targeted. Effective proactive engagement requires considerable preparation to adapt the narrative to the agenda of the government official you are meeting with.

Most of the work done in the first phase of a marketplace is reactive, not proactive. Companies often find it difficult to be proactive until they have sufficient resources. The advantage of this form of work is that you can include the voices of your users in important conversations. When new regulations are introduced that could put your business or users at risk, it's crucial to be involved in the discussion and track the progress of the legislation. When you're responding reactively, it's important to thoroughly assess the pros and cons and have a broad view of your business in mind. You want to avoid the risk of losing customers, contracts or engagements. You should weigh your options and think about using other sources of support - such as signing a letter or waiting for things to unfold before making a statement. You can then plan a few steps in advance to approach the situation.

Insight NO. 4:

ADA Website Accessibility: What Every Platform Must Know About Compliance

Sandra Dainora
Director of Public Affairs
Sittercity

Michele Landis
CRO &
Co-Founder
Accessible360

Kristina Launey
Labor and Employment Litigation and Counseling Partner
Seyfarth Shaw LLP

An estimated 61 million US adults have some form of disability, making compliance with the Americans with Disabilities Act (ADA) crucial for marketplaces. The ADA covers four main disabilities - visual (which includes low vision and color blindness), cognitive, physical and auditory.

When the ADA was signed into law in 1990, the internet wasn't yet developed, so there's disagreement about whether the legislation was applicable to websites and the internet in general. We've received guidance through case law since then, but courts disagree resulting in significant litigation. Generally speaking, if a company provides goods or services to the public, then Title III of the ADA applies. But there's no standard in the statute or the regulations that says your website must be coded or look a certain way.

There's been dispute over whether Title III applies to digital-only businesses that don't have physical spaces, this issue is still being litigated and rulings vary depending on the court. The ADA requires that businesses provide auxiliary aids and services at no extra charge that might be necessary to ensure effective communication with individuals with disabilities. While there's a list of types of services and auxiliaries required, it doesn't include websites specifically, but it does say "accessible electronic information technology" which has been interpreted to include websites, mobile apps and other digital technologies.

What happens if you get sued? In the event of a lawsuit, the plaintiff is eligible to receive a court-ordered directive to fix any violations. Additionally, if the plaintiff takes legal action against the defendant under state statutes such as California's UNDERREACT, they may receive monetary compensation for attorney fees, court costs, penalties, and/or damages. The Department of Justice (DOJ) can also impose hefty fines and even expand their investigation to other aspects of your business. The number of lawsuits related to Title III of the ADA have continued to rise each year, reaching over 11,000 lawsuits in 2021 alone. And the problem is larger than it appears as only one in one hundred demand letters turns into a lawsuit. With demand letters requiring a response that still impacts a business.

The de facto standard for website accessibility is the Web Content Accessibility Guidelines (WCAG) 2.0 and 2.1, particularly the AA Guidelines. Regardless of the expert hired, they'll use the WCAG to determine if the website is accessible or not. The DOJ issued some guidance a few months ago, essentially suggesting that the WCAG guidelines should be taken into account.

Insight NO. 5:

Understanding and Preventing Fake Online Reviews

Jeff Chugg
Global Head Risk and Response
TaskUs

Kevin Lee
VP Trust and Safety
Sift

A few years ago, Dictionary.com called misinformation their word of the year. Today, with the abundance of information available online, it can be tricky to discern fact from fiction. We know that for marketplaces, quality interactions drive growth. So, naturally, fake reviews lead to a decline in engagement for legitimate users, and ultimately cause them to leave the platform. Anyone who's come across a product that didn't meet expectations based on misleading reviews understands the frustration it creates. The real danger of fake reviews is the loss of consumer confidence and trust in the marketplace. And these negative end user experiences can spread and damage an entire platform. It's a large and rapidly growing problem. If you're responsible for risk and compliance, and for keeping a platform free from fake reviews, it can be overwhelming due to the sheer volume of scammers.

We've conducted studies to determine how fake reviews are coordinated. Our research suggests that fake reviewers focus their efforts on specific price points and product categories. If there's a common theme, it's products priced at $50 or less within the following categories: automotive, beauty & personal care, apparel, jewelry, electronics, home & garden, sports, outdoors, tools, home improvement, toys, and games. We believe this is because it's easy to get someone to order the item, write a review, and then return it or buy it back from them if it's low cost.

People who post fake reviews may not know what they're doing, which is shocking given they receive instructions to purchase and return an item and provide a five-star rating with specific key terms. These fake review groups also provide instructions to avoid detection by algorithms such as mispelling words, or using a "3" instead of an "e". In one marketplace that we reviewed, 90% of the sellers participating in these schemes were located in China, while the remaining 10% were scattered throughout Germany, Great Britain, the US, Hong Kong, Singapore, and unknown locations. Other platforms have fake review groups originating from Bangladesh and Turkey.

In our analysis of 100 public Facebook groups that recruit fake reviewers, we found that 47 of these accounts were created in 2021, which is nearly equivalent to the number of accounts found from the previous five years combined.

It shouldn't be a surprise that one-hundred percent of fake reviews are five stars. Many of us have reached the point where we naturally distrust five-star reviews. Oftentimes, these reviews are posted close to one another and in a short period of time. This can be a useful indicator to look out for when shopping online or monitoring your platform and trying to distinguish between real and fake reviews. According to the research, 75% of reviews posted close to one another are fake, along with 60% that contain generic phrases such as "good quality" and "looks great".

Insight NO. 6:

Data Privacy, Legal, & Bias: Ethical Considerations with Leveraging AI

Jonas Bordo
CEO & Co-Founder
Dwellsy

Kathleen McConnel
Partner
Seyfarth Shaw LLP

The data protection, legal and ethical considerations of artificial intelligence (AI) on platforms are a growing concern. When we refer to AI, what do we mean? We're focusing on two primary categories. One is where you use a logic tree to pre-program decisions. The other model, which has gained popularity in recent years, relies on machine learning. Machine learning involves a set of rules that are programmed, but the software takes over and makes decisions and connections on its own based on those rules.

The ways we see AI being used across different platforms and programming are to draw conclusions, make informed judgments, optimize existing practices, and automate repetitive tasks. For example, there's a marked increase in AI use in the recruitment and hiring process. AI is being used to detect suitable candidates and vet the candidate pool. It's also used to schedule interviews, refine job descriptions, and answer inquiries from applicants via chat bot. Video interviews are increasingly popular, with AI involved in various aspects of the process. With the rise in remote workers, there's also remote monitoring tools that rely on AI along with dash cams and telematics.

And many of the tools we use, like LinkedIn for recruiting, use AI, but we don't know how exactly. How does it narrow down the candidate pool? This is a crucial consideration, how do the tools we use leverage AI, and what are the implications behind that?

AI is a key element of the modern SaaS tools utilized for workforce management. These tools are used from the moment a candidate applies for a job to the last day of their employment with an organization. However, the interactions between employees and those tools are often unknown or not well understood. This can lead to a situation where the employee experience is vastly different from the employer's view, presenting a high degree of complexity and risk for the organization.

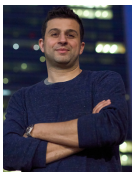
From a legal point of view, AI has presented challenges in the workforce related to disparate treatment and impact. Disparate treatment is where people are treated differently due to their membership in a specified class, while disparate impact is when policies or practices have an unequal influence on members of a certain group. AI is generally seen as a beneficial tool, as it can be used to reduce conscious and intentional bias when selecting employees. Furthermore, when functioning properly, AI may also help increase workplace diversity.

Some of you may recall that Amazon had to discontinue its AI-driven recruitment platform a few years ago. After dedicating several years to the development of this system, they soon discovered it was rating women applicants lower than other candidates. After further investigation, they discovered that the primary data used to train the tool were the profiles of successful people they had already hired, who were predominantly male. This highlights the importance of keeping an eye out for bias when AI is involved. If the data used to train the tool is biased, future results will be too.

Insight NO. 7:

Reduce Fraud and Increase Trust Through Digital Content Verification

Judith Germano
Founder
GermanoLaw LLC



Mounir Ibrahim
VP of Public Affairs and Impact
Truepic

Andrew Kaback
Sr. Product Manager
Adobe

As the amount of digital content grows rapidly and the risks of fraud and deception multiply, it's important to protect ourselves from falling prey to manipulated images and videos. Hundreds of millions of images and videos are uploaded to the internet every day, but not all are verified or vetted. This brings up some serious trust and verification issues.

Trust in imagery is dropping, as reported by the Edelman Trust Index. To tackle this issue, Data and Society released the Spectrum of Fakery, a tool to better understand the distinction between cheap fakes and deep fakes. A cheap fake is something as simple as changing a caption or altering the color of a photo, while a deep fake is a wholly synthetic video. The trouble with fakes is they can be used for fraud and deception, which presents considerable risks for businesses and individuals. To make informed decisions, the public needs to know what's real and what's fabricated.

Recent data from the FBI shows that business email compromises have resulted in over $43 billion in losses since 2016. This is just one example of significant fraud, but it's clear that businesses must take measures to ensure that the people and entities they're transacting with are who they say they are.

Identity verification plays a major role in this effort. Companies must take the time to verify identities and ensure that the people accessing their systems are authorized to do so. This is especially true when sending money, as many people have become victims of fraud by wiring funds to the wrong person. Businesses should also be proactive in securing their data and information. It's no secret that fraudsters are always searching for new ways to get their hands on sensitive information. Companies must put the right measures in place to protect their data and ensure it isn't compromised.

Financial compliance is essential for any business, and regulators increasingly require companies to take measures to prevent fraud and money laundering. Verifying customer identities and conducting Know Your Customer (KYC) and Anti-Money Laundering (AML) checks are key components of this process. Organizations must quickly and accurately assess customer data to ensure compliance with laws and regulations. This isn't an easy task, as advances in technology have made it easier for criminals to commit fraud and launder money. Companies must take extra measures to ensure the data they collect is accurate and up-to-date. This includes developing robust customer identification systems, incorporating analytics to detect suspicious activity, and implementing a system to monitor the flow of funds. In addition, companies should ensure their customer databases are secure and have effective processes to monitor and detect suspicious transactions. Compliance is essential for any business, and it's important for companies to have the tools and processes in place to ensure they meet their legal and regulatory obligations.

Insight NO. 8:

How Marketplaces are Being Leveraged by Fraudsters: The Most Popular Scams

Filip Verley
Group Product Manager
Google

Amy Walraven
Founder & President
Turnkey Risk Solutions

With digitization reaching an unprecedented level, it's essential that everyone - individuals, businesses, and even the government - be aware of the various types of fraud that exist. Third-party fraud, which many people are familiar with, occurs when a customer is victimized (such as identity theft, counterfeiting or account takeover). First-party fraud has become more widespread in recent years. This occurs when a bad actor deceives an institution, and the business becomes the victim. This type of fraud can lead to financial loss, credit damage or regulatory exposure.

Prior to the pandemic, the fraud landscape focused largely on social media, where people were misled by various phishing techniques. For example, asking questions such as a person's favorite food or the make and model of their first car. This information can then be used to compromise someone's security questions to gain access to their accounts.
The pandemic accelerated digitization, resulting in a surge of new customers starting transactions online. Traditional data sources are, therefore, no longer reliable, and knowledge-based authentication (KBA) is not as effective. Companies need to find new ways to determine who can be trusted online, and this is an area that still needs significant improvement.

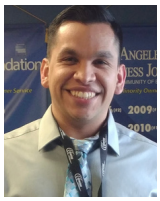
The current state of social media and the pandemic have dramatically changed the fraud landscape. It's now more important than ever for individuals and businesses to be vigilant when it comes to protecting their digital identities and transactions.
Synthetic identities have become a common occurrence in the financial services sector. This refers to the creation of an identity that emulates a real person using someone else's personal information, such as their social security number. This can be used to hide negative records and allow someone to qualify for services they wouldn't be able to access under their real identity. Synthetic identities have been used in the ride-share industry to cover up a criminal past or suspended driver's license. The use of synthetic identities also creates an exposure risk for property owners, who might unknowingly facilitate organized criminal activities or money laundering. In the food delivery industry, scammers have been known to scan customers' licenses and commit identity theft. This highlights the difficulty in dealing with scams in marketplaces.

Losing customer confidence can be difficult to regain, especially in a highly competitive market. The cost of combating fraud can also strain a business's resources and affect their profit margin. The impact of brand and reputational risk cannot be quantified, but it can make or break a business.

Insight NO. 9:

Game-Changing Trust Techniques Used by the Largest Marketplaces

Netta Abres
Group Product Manager
Identiq



Emilio Lopez
Senior Strategy and Data Analyst, Fraud Prevention
Newegg

Trust is a crucial aspect of online services, but it's often difficult to achieve. Customers need to know that their personal information is secure, especially when conducting transactions with people they don't know. To ensure that customers feel safe and secure, marketplaces must prioritize identity verification while also providing an excellent customer experience. This involves navigating the delicate balance between experience and security.

Unauthorized access to customer data can lead to financial losses and reputation damage, so organizations must protect customer data to the highest degree possible. It's important to regularly monitor customer activity to detect any breaches. It's also necessary to introduce a secure authentication process, such as two-factor authentication and encryption, to protect data in transit. Customers expect a seamless experience when visiting a website or using a product or service. Marketplaces must reduce friction and make the process as smooth as possible. This can include streamlining the checkout process and ensuring that customers quickly and easily find what they need.

Privacy-enhancing technology (PET) is becoming increasingly well known. PET is a well-established and extensively researched field of technology that allows individuals, institutions and companies to collaborate and share information without having to disclose personal or sensitive data. This removes the role of a third party or intermediary, enabling a company to validate its customers' data without having to access their private information.
PET is used in many industries, including the financial and banking sectors. It allows companies to verify customer information upfront, such as email addresses, phone numbers and credit card details. This ensures customers trust the services provided, as the data exchange is secure and private. Other companies use PET to facilitate collaboration between departments, such as customer service and sales, as well as the underwriting team.

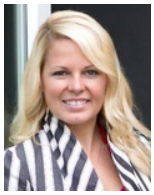
The introduction of privacy-enhancing technologies enables companies to keep their customers safe and secure, and is an invaluable tool to ensure that sensitive data is kept private. The fraud prevention industry is built on trust. Collaboration between industry professionals is crucial to stay one step ahead of fraudsters, who often work together on the dark web. This collaboration should include the creation of an approved and declined list. The declined list can help prevent fraudsters from slipping through the cracks, while the approved list can help enable sales by trusting the right people.

The current system of sending data to third-party providers and trusting them to indicate good or bad actors is fraught with problems. These issues range from stale data and data theft to privacy protection. To address these problems, companies need to work directly together, rather than rely on third-party vendors. This can help ensure data freshness, protect against data theft and leaks, and reduce the risk of exposure. By working together and creating a more secure system of data sharing, the fraud prevention industry can ensure trust between professionals and protect the interests of all involved.

Insight NO. 10:

How to Recognize and Eliminate Fraud in Your Marketplace

Jonas Bordo
CEO & Co-Founder
Dwellsy



Candace Sjogren
VP of Emerging Markets
Socure

Promotion fraud and rewards abuse are a major problem that many marketplaces face today. This form of fraud involves the use of fake accounts and promotions to take advantage of the rewards or incentives offered by the marketplace, resulting in losses for the company. Rental fraud is another problem that has grown steadily in recent years, driven in large part by the rise in counterfeit listings. The traditional method of renting a property, such as on Craigslist, is no longer the primary method, as more fraudulent listings have emerged. Individuals have become more professional in their attempts to cheat the system and set up elaborate schemes and scams to make a profit.

This has caused significant disruptions in the rental market, and individuals can no longer trust the listings they find online. To combat this, companies have developed advanced systems for analyzing data points related to rental transactions to detect fraudulent activities. The data analyzed includes changes to the customer's email, address information or other behavior considered suspicious or out of the ordinary. This is an example of how advanced technologies, such as AI and machine learning, are being used to create more secure and reliable marketplaces. This technology is also being applied to other industries, such as finance and banking, to help prevent fraudulent activities and protect consumers.

Identity verification is becoming increasingly important for online marketplaces. Platforms should start identity verification (IDV) at an earlier stage of the process, before payment and before counterfeit products are listed. Doing so can protect against fraud, risk, and ensure fairness and inclusion. To comply with regulatory and contractual obligations, platforms must implement a 'Know Your Customer' (KYC) procedure. This requires platforms to build an 'identity graph' to protect against potential risks and ensure fairness to all customers. Fair Housing laws make it illegal to consider certain characteristics when renting out property, such as race, gender or ethnicity. As such, marketplaces need to ensure that the identity verification process is fair and impartial.

This means the process should not involve biased decisions, and should not involve manual processes that could lead to discrimination. Platforms must also ensure that the IDV process is transparent, allowing customers to view and understand the procedure in a simple and easy-to-follow format. Ultimately, identity verification is an important part of the online marketplace process. By implementing a KYC process that's fair, impartial, and transparent, platforms can ensure that fraudulent activity is minimized, and fairness and inclusion are promoted.

Insight NO. 11:

How to Stay Ahead of Fraudulent Sellers

Mindy Kasting
Product Lead, Platform Risk
Adyen

Kevin Lee
VP Trust and Safety
Sift

Sandi Liu
Payments Risk Product Manager
Google

Fraudulent activities by bad actors have become a growing concern for marketplaces. Despite efforts to onboard legitimate users and verify their identities, studies have shown that up to 3% of sellers on a platform engage in some form of fraudulent behavior. And multi-sided fraud is particularly widespread, where both buyers and sellers are in the mix. This can put up to 6% of a marketplace's revenue at risk, and can lead to as many as 60% of users avoiding future interactions with the platform. Bad actors can target a platform in several ways, including account acquisition, fraud rings that collect credentials, and synthetic fraud. Synthetic fraud is when someone's social security number (SSN) is stolen, and then other information, such as name, date of birth, mailing address, email account and phone number, is created and applied to this legitimate SSN to create a new identity.

In addition, bad actors can also be sellers who register on the platform to engage in fraudulent activities. Many marketplaces have individuals and teams dedicated to risk management and protecting their customers and consumers from these risks. It's essential that these companies continue to stay ahead of the curve in detecting and preventing these fraudulent activities, in order to maintain the trust and safety of their platform.

Collusion is also a growing concern for marketplaces and e-commerce platforms. This practice involves merchants using stolen credit cards or fraudulent means to buy from their own store, pumping up their sales figures and artificially increasing their popularity. This can be done through a single transaction or a more complex web of relationships between buyers and sellers. Marketplaces must be vigilant in detecting these relationships and identifying clusters of activity that may indicate illicit behavior.

One type of collusion is known as buyer-seller collusion, in which merchants buy from themselves with their own money and then refund themselves. This allows them to earn loyalty points or sign-up bonuses, which can then be used elsewhere. To detect such activity, marketplaces must look at the history of buyers and merchants, including the length of their relationship with each other and the marketplace, and the pattern of their transactions. Another form of collusion is triangulation, in which a buyer makes a purchase through a marketplace, but the actual transaction takes place elsewhere, often through a different payment method. This can make it difficult for the marketplace to detect fraudulent activity, and lead to chargebacks and disputes that negatively affect the platform and its legitimate users.

The rise of online marketplaces and the shift to online commerce have created new opportunities for illegal activity. Marketplaces must be aware of these trends and work together through data exchange consortiums to combat them. By taking a proactive approach to detecting and preventing collusion, marketplaces can maintain the trust of their customers and the integrity of their platform.

Insight NO. 12:

Speed to Marketplace: Onboarding Safely Within Minutes Not Weeks

Jevin Bhorania
Sr Director of Risk and Data Science
Faire

Jag Lamba
Founder & CEO
Certa

Patrick McConville
VP of Bus. Dev.
Certa

Yuvika Rajan
Sr. Manager, NA Sales Engineering
Mitek

Effective onboarding is crucial for marketplaces, and is a high-stakes, high-friction process that requires care and attention. A well-structured framework can help companies reduce risks and operate more efficiently. The typical onboarding process is plagued by problems such as massive delays, inefficient internal processes and high friction. As a result, it often leads to frustration among internal users, such as sales teams, who want to sign up new clients, but can't get the information they need to do so.

One of the biggest roadblocks companies face during onboarding is the risk of fraud. According to recent data, 72% of consumers won't use a marketplace with a reputation for fraud. Add to that, too much friction during the identity verification process can also discourage customers from using a marketplace. This creates conflicting priorities for platforms that need to balance the risk of fraud with the risk of high friction.

In today's digital landscape, avoiding fraud while maintaining a seamless user experience is a top priority for marketplaces. To effectively combat fraud and protect against financial losses, it's essential to establish a continuous feedback loop by analyzing user behavior and identifying fraud trends. However, this must be done carefully, as too much friction can have a negative impact on the user experience and conversion rates.

Complex interpretations by compliance teams of what constitutes a robust Know Your Customer model can also pose challenges. To address this, a layered approach is recommended, starting with a basic model and building on it while the user explores various services and offerings. It's also important to be in sync with the finance and growth teams to ensure friction is added at the right thresholds to maximize the customer's lifetime value. Visibility and transparency are also key factors for optimizing the fraud prevention process. Capturing data and providing insights into the process can help all stakeholders understand who's doing what, while identifying bottlenecks that may require additional resources.

One aspect that plays a crucial role in the success of a platform is the use of signals collected during the customer onboarding process. These signals are used to influence the decision-making process and can determine whether a customer should be automatically approved, sent for manual review, or given additional prompts. The data collected when onboarding new customers, combined with the analysis of a customer's behavior on the platform, can provide valuable insight into the customer's intentions and preferences. When it comes to setting up a process to manage customer acquisition, it's important to remember the need to future-proof the program. This involves selecting solutions that are flexible and easily adaptable, so that new APIs and data can be integrated as they become available. In this way, the program remains relevant and up-to-date, even as new risks emerge.

Insight NO. 13:

ESG for Beginners: What You Should Know about Developing an ESG Strategy

Kevin Feldis
Partner
Perkins Coie LLP

Heather Lewis
Director, Community
DISCO

Environmental, social and governance issues (ESG) are becoming increasingly important for marketplaces and platforms to consider in their operations and decision-making. This is not only in line with the expectations of users and other stakeholders, but also has the potential to increase value, minimize risk and strengthen the company in the long term.
ESG is composed of three parts: environmental, social, and governance. Environmental refers to your impact on the environment, including emissions. Social encompasses your supply chain, the treatment of employees, and other related factors. Governance covers your code of conduct, ethics, governance structure and diversity of participation.

Integrating ESG principles into business strategies is not only a matter of social responsibility, but also a requirement under corporate law in many jurisdictions. Companies are increasingly expected to take into account all stakeholders, including employees, customers, suppliers and the communities in which they operate, as they make decisions and formulate policies. One way to establish an ESG strategy is to follow the four principles of governance, people, the planet and prosperity, outlined by the International Business Council of the World Economic Forum. You might think, “How does that apply to me? My business isn't a large platform that consumes a lot of energy, so this must not be important for my company.” These principles provide a framework for all companies (large and small) to assess their impact and take measures to improve their performance in areas such as reducing emissions, improving working conditions and promoting sustainable economic growth.

Many large organizations have already taken a stand on ESG issues and are leading the way in their respective industries. For example, some companies have formed partnerships with organizations that align with their brand values and help support important causes. By taking such steps, companies can connect with their customers, differentiate themselves from their competitors, and build a strong reputation.

As a growing platform, the adoption of ESG goals can bring many benefits and help you differentiate your platform from others. Investing a little in ESG now can offer a great return on investment in the future, strengthen your business, mitigate risks and increase the value of your business. An ESG strategy can also help you build resilience, attract investors and increase the value of your business. It may also cost you more in the future if you aren't up to speed on ESG initiatives. To start, analyze and consider how ESG fits in with your business by identifying a few ESG-related priorities and assign one to focus on in the categories of environmental, social or governance. It's important to think about your ESG goals, not only because it's the right thing to do, but also because it will have a positive impact on your business.

Insight NO. 14:

Everyone is a Data Scientist: How Non-Technical Teams Can Improve Customer Experience by Leveraging Data

Trisha Kothar
CEO & Co-Founder
Unit21

Unit21

Data science has been a hot topic in recent years and is becoming increasingly accessible to all. As more and more non-technical teams begin to use data to improve customer experience and solve trust and safety problems, the importance of data science continues to grow. The challenge of fraud detection and prevention is one of the key areas companies have focused on. Despite the high volume of vendors on the market, more effective solutions are still needed. The market for fraud detection and prevention is expected to reach $75 billion by 2028, which underscores the importance of finding a better solution.

People's fears of identity theft and financial fraud are even greater than their fears of being murdered, highlighting how crucial this issue is to consumers. Despite the many solutions in the space, something is still fundamentally missing. To better understand this, it's important to look at the growing problem of romance fraud.

Over the last five years, more than 1.3 billion cases of romance fraud have been reported to the FBI, with more than half a billion of these cases occurring in 2021, alone. Dating companies use a wide range of solutions to detect fraud, but the problem continues to escalate. In 2021, $139 million of the $550 million lost in romance fraud was lost to cryptocurrency, an area of the financial world that lacks clear regulations and controls. Military romance fraud, in which individuals claim to be in the military and ask for money, is another growing vector of fraud.

Data science plays a crucial role in ensuring the trust and security of transactions for platforms. This includes three key components: data extraction, collection and cleaning; the creation and testing of a hypothesis; and the use of data labels on production models. The aim is to use all of a company's data, including internal data, that cannot be fed into third-party risk values by third party vendors.. This is because these providers collect only limited data, and the models are trained only on a small subset of data, not all available data. To create a hypothesis, teams must test proposed rules before they deploy them, and this requires engineering bandwidth and getting all the data into one place. There are two effective methods for testing rules: testing rules based on historical data and conducting AB tests using multiple data parameters. The goal is to see if the rules are effective, what the operational burden would be, and whether they’re doing what's intended.

For example, a company like eBay might want to see if the auction item type is a Rolex watch, and then change the parameters to see how it affects the data. By continuously evolving models based on new data and feedback from operations teams, marketplaces can ensure the trust and safety of transactions on their platforms.

Insight NO. 15:

The Next Frontier in Identity Verification: Unpacking the Digital Identity Wallet

Taylor Liggett
General Manager
Sterling Identity

Mark Lockwood
Chief Revenue Officer
Wowza

In the digital age, the concept of a reusable or portable identity is becoming increasingly important. The idea that individuals have control over their own information and identities is becoming increasingly common in the industry. In fact, companies are creating digital wallets for the identities of individuals that allow people to control and carry their information, like a financial information model.

The digital credentials offered by these companies include digital driver's licenses, military verification, and professional credentials such as nursing licenses. The focus of these solutions is consumer-oriented, empowering individuals to control their information and making it portable. Fraud is impacted by the environment. For example, the pandemic led to an increase in unemployment benefits, and with it, a rise in employment fraud. Legacy systems within government agencies were the main targets for bad actors. They saw the ease of creating fake identities, which was more profitable and less dangerous than other illegal activities they had previously engaged in.

During this time, the value of a network-based approach, versus a transaction-based approach, was realized. With a network-based approach, it was easier to see fraud migration across different state unemployment systems. The bad actors applied for unemployment benefits in several states, and a network-based approach helped highlight these illegitimate claims by better understanding the scope of their activities.

Criminal enterprises have made significant investments in identity fraud and have become increasingly sophisticated in navigating the system. The increase in remote work and the ability to steal identities has only added to the problem. Identity verification and data protection standards are crucial for financial transactions, and a digital wallet can streamline these processes and simplify the verification process. Identity verification and data protection standards are key aspects of financial transactions. The stringent requirements imposed by the IRS to access tax returns are a testament to the importance of these standards. A digital wallet is the solution for streamlined transactions and simplifies the verification process. The idea behind this concept is that if a person can protect their data and validate their identity for the IRS, the same standards can be applied to commercial transactions.

Digital wallets have the potential to be a limitless and versatile tool. The focus has been on group verification and streamlining repetitive screening initiatives. However, the extent to which a digital wallet can be used is only limited by the trustworthiness of the source. Verified information and credentials can be linked to an individual's identity, and the process can be even easier through QR codes or other check-in mechanisms.
Some companies are interested in using digital wallets to offer benefits and discounts to certain demographic groups, such as military personnel or contractors, with the assurance that the information is verified and secure. The development of digital wallets has a lot of promise, but also challenges. Legal identity verification is one of the biggest challenges, but the possibilities of this technology are endless.

Insight NO. 16:

Staying Ahead of Online and Marketplace Tax Obligations with Automation

Liz Armbruester
SVP, Global Compliance
Avalara

Avalara

Marketplace providers, businesses, and sellers must take compliance seriously when it comes to taxes. Maintaining compliance is difficult, as the US has 13,000 regulatory agencies alone that change their minds daily. The challenge grows when facilitating sales for sellers that move across borders, requiring knowledge of each country's regulations. Furthermore, compliance varies for each type of business, whether it’s tangible personal property, services, or something else.

In June 2018, the US Supreme Court in South Dakota v. Wayfair expanded the ability of state and local governments to impose taxes on remote businesses. It did so by replacing the nexus standard of "physical presence" with "economic presence," i.e. the amount of economic activity occurring in the state. Alongside this came the Marketplace Facilitator Act, in which marketplaces were suddenly responsible for collecting, filing and remitting sales taxes on behalf of their sellers.

While some states don't tax certain types of services, it's important to stay up-to-date on laws and regulations, as they shift frequently. This is especially true for digital services and goods, which are a rapidly growing sector of the market. One question that often arises is who’s responsible for remitting taxes, the seller or the marketplace? The answer is that the marketplace typically pays taxes on goods sold on its platform. However, sellers may still be responsible for remitting their own taxes for brick-and-mortar sales.

It's important for marketplaces to keep accurate records of sales and taxes collected and remitted. This information can help companies comply with tax laws and regulations, and provide an audit trail in the event of discrepancies or legal issues.
As the world becomes more digital and transactions are carried out around the clock, tax authorities are increasingly interested in accessing data in real time. While tax reporting currently operates in a post-period environment in the US, where transactions are reported after they occur, transactions are approved and cleared by the government before they even occur in other parts of the world.

Businesses have an obligation to ensure they follow tax laws and regulations, which is where tax professionals come in. They can help companies stay up to date with the latest tax laws and requirements, as well as help with tax reporting and remittance. In addition, due to this growing complexity, tax automation software is an approach that marketplaces should also consider. Tax automation software is like a self-driving car, in that it enables more control than businesses have on their own. The software helps companies pay their taxes accurately and faster, and gives them a high degree of confidence that everything is done accurately and on time.

Insight NO. 17:

The Hazards Of 1099'ing Your Platform: How to Successfully Leverage Contractors in Today's Regulatory Environment

Phillip Ebsworth
Associate
Seyfarth Shaw LLP

Seyfarth

Pamela Vartabedian
Partner, Labor & Employment
Seyfarth Shaw LLP

Seyfarth

As businesses increasingly rely on independent contractors for flexibility and cost-effectiveness, proper classification has come to the forefront. Misclassifying workers can lead to significant liability, including back taxes, penalties, and even lawsuits. It's particularly important in California, where the standards are strict. States rely on different tests to determine whether a worker should be classified as an employee or independent contractor. Some states use the Common Law Test, a multifactor test that weighs various criteria to determine whether there is an employment relationship. The ABC test, which is used in many states, including California, is a more rigorous test that requires a company to meet three specific criteria to classify a worker as an independent contractor.

Classifying someone as an independent contractor is not a decision that can be made simply by providing a 1099 form. There is more to it, and any misclassification poses a significant risk to employers. Studies have shown that between 10% and 15% of employers misclassify at least one employee, and that's probably an underestimate. Whether intentional or not, misclassification is a crime that can lead to significant financial penalties and in some cases serious legal action. Companies must be careful when it comes to classifying workers as independent contractors. It's a good idea to ensure that they meet the criteria set out in the ABC test. It’s also recommended to seek legal advice to review these practices and ensure compliance with state and federal laws.

When it comes to classifying workers as independent contractors, with the ABC test, there are three factors. Factor A is that they are free from the control and direction of the marketplace, meaning they direct their own work. Factor B is that if the work is carried out outside the usual course of the employer's business, it's easier to classify the worker as an independent contractor. For example, if you hire a plumber to come in and fix something, assuming you are not a plumbing company, that would be outside the scope of normal business. However, this is typically the hardest prong to satisfy for marketplaces.

The third aspect, or factor C, that determines whether a worker can be classified as an independent contractor is whether they have their own independent business or trade that does this type of work. Ideally, the worker has a formal program or does similar work for other clients. All three factors must be satisfied to classify someone as an independent contractor. Factor B is often problematic for companies. Some marketplaces have argued they are a platform company, not in the business of providing transport or other services that workers provide. However, at least one California appellate court has not accepted this argument. The court ruled that the workers made all the money for the company, and that the company could not be in business if it weren't for those workers.

Insight NO. 18:

Top Five Trust & Safety Trends for Marketplaces in 2022

John Greene
Vice President of Marketplaces
Prove

Reddy Karri
CEO
Vetty

Onboarding innovation, ID verification, AI and machine learning, industry consolidation and expanding services are the five top trust and safety trends that dominated 2022. Onboarding innovation is the first trend on the list. Visual onboarding has continued to make the process better, faster, and with less fraud. However, the biggest friction point for candidates is the tedious data collection and documentation required. Traveling nurses, for example, can have up to 30 addresses, while drivers applying for multiple jobs must repeatedly enter the same information. To solve this, some background check companies now only collect the mobile number and partial PII information. The system then pulls in all the candidate's information, which they just need to review and verify. This solution has already received positive feedback and has sped up the whole process.

The second trend is ID verification, which is part of the background check process. Previously, data collection was more like uploading a document, and most candidates saw their IDs fail, causing delays. Mobile ID verification is now being used to help candidates with low-quality documents, making the process faster and more convenient. The third trend is the rise of AI and machine learning. More companies are using automation to reduce fraud and minimize false positives. Automated risk assessments and predictive analytics are becoming more popular, and can now identify threats and suspicious activities faster than humans. The fourth trend is industry consolidation, with more companies merging or being acquired. This trend is also helping to streamline the background check process and make it more efficient for both clients and candidates.

The fifth trend is expanding services. Background check companies now offer more services, such as identity verification and fraud prevention, which they believe are the next big thing in the industry. Platforms are looking for more efficient ways to manage their security risks, and background checks and several providers are well positioned to provide these services. Continuous monitoring of employees is an important aspect of risk management, but not all employers do it. Although background checks are typically carried out before employment, ongoing monitoring is often neglected. This is a risky approach, because even if a candidate's background check is clean, it doesn't mean they won't commit infractions after joining the company.

In addition to monitoring, behavioral biometrics is an interesting technology that can be used to determine an individual's authenticity and identity. This technology can passively understand how someone uses their device, including how they type, interact with their phone, hold it, and walk with it in their pocket. The technology can also identify the types of environmental signals around the individual, such as the Wi-Fi they typically use, or whether they have their car Bluetooth on when checking in for a shift. This can be used to passively authenticate the individual without requiring them to do anything. As technology continues to evolve, background check companies are well-positioned to offer more innovative and efficient solutions to their clients.

Insight NO. 19:

Leveraging Technology to Enhance Trust & Safety and User Experience

Chris Aragon
Sr. Director, Risk Management
Getaround

Hamed Yazdi
Chief Growth Officer & Co-Founder
Rideshare Mechanic

As the mobility industry continues to expand, managing risks becomes increasingly important. Safety concerns and financial implications are just a few of the risks that companies must navigate to protect their brands and customers. One approach to reducing friction in the onboarding process for drivers is to offer certified vehicle inspections conducted over video chat. This method has proven effective for companies serving both business-to-consumer and business-to-business marketplaces, including peer-to-peer platforms and non-emergency medical transport. Another approach to mitigating risk involves understanding acceptable risks and the company's tolerance level. By focusing on claims and premium costs, as well as every customer interaction, to build brand affinity and goodwill capital, companies can protect their brands and customers and ensure their financial stability.

While the risks in the mobility industry are large, many companies have developed effective strategies to mitigate them. By embracing new technologies and methods that improve the user experience and challenge long-held assumptions, companies can continue to improve their processes and stay ahead in a competitive market. For example, virtual inspections with owners rather than in-person inspections by mechanics may seem less effective than traditional inspections, but the data proves that participation of the car owner in the virtual inspection can lead to better quality and more traceability. Companies should therefore review data before deciding whether to implement new technologies or processes.

Another example is vehicle age. Older vehicles were not previously considered part of the risk strategy of many car share companies, as newer cars were believed to have fewer breakdowns and better performance. However, the data showed that many older vehicles are well maintained and as reliable as newer vehicles. They also offer more economical rental options for people who can't afford the fees imposed by newer models. To mitigate the added risk of incorporating older vehicles, you can adjust the criteria and require inspection by a mechanic after a certain production year. It’s also essential for marketplaces to establish a culture for trust and safety teams to prioritize risk mitigation in every initiative they work on. An effective way to do this is to highlight the importance of the work and its impact on the protection of the company and the promotion of positive brand experiences. In addition, building internal incentives without external motivation to conduct or fail inspections can be beneficial.

More importantly, it's essential to recognize the importance of the job and continually remind the team of their responsibility to create a safer world. This can be achieved through company meetings and calls that emphasize the importance of the work in ensuring people's safety. Transformative changes in a platform's processes can result from being open-minded, playing the devil's advocate, and using data to make decisions. By challenging assumptions and embracing new technologies, marketplaces can improve the user experience and mitigate risks.

Insight NO. 20:

Staying One Step Ahead: Bad Actors and Your Brand

Eric Levine
CEO & Co-Founder
Berber

Berbix

Protecting your business from fraud is crucial for running a successful marketplace. Understanding fraud and the various types of bad actors is the first step in combating it. With nine out of 10 Americans experiencing a fraud attempt and $42 billion lost in fraudulent activities over the past two years alone, platforms must act urgently and take the necessary precautions to protect their users and customers. There are three types of bad actors: premeditated, opportunistic, and accidental. Premeditated bad actors come to your platform with the intent to commit fraud and get the most attention.

Opportunistic bad actors are generally good users, but take advantage of the opportunity to commit fraud. Accidental bad actors violate platform standards unknowingly. Understanding these types of bad actors and the various fraudulent activities they engage in can help your team develop effective fraud mitigation techniques. Companies should consider fraudsters as a business, and less as criminals, to prevent fraudulent activities. Fraudulent activities can take various forms, such as account takeovers, identity theft, fake accounts and chargebacks. By understanding these types of bad actions and the different types of bad actors, businesses can strengthen their defenses.

Given the increasing number of data breaches and online fraud, companies must take identity verification seriously. Various methods of identity verification, such as email and phone verification, are widely used, but they're not strong enough to keep bad actors off a platform. Many companies are turning to more robust identity verification methods, such as mapping a person in the digital environment to the person in the real world. Government-issued photo IDs are widely accepted tokens that represent a person's identity in government systems. This tool is an effective way to identify a person when they create an account on a platform, and ensure that the same person returns to the platform later.

In addition to identity verification, platforms are investigating other signals to detect fraudulent activities. However, the most effective and high-quality information about a user still comes from an ID, which is the best way to obtain user information. Companies can also incorporate probabilistic patterns to slow down bad actors when attempting to reverse engineer protections.

Clear expectations and consequences should be set for those who violate the platform's standards. For premeditated bad actors, making it unprofitable for them to attack the platform is crucial. Companies can achieve this by ensuring that the potential loss to bad actors is greater than the potential gain. Finally, it's important to address accidental substandard users. Educating users and warning them when they violate the platform's standards is essential in preventing fraud. By doing so, companies can ensure that users understand the consequences of their actions and make informed decisions.

About Marketplace Risk

We began as a working group of founders and executives from diverse marketplace startups, who came together to explore best practices and learn how to better identify and mitigate the risks associated with our platforms. Over time, our group has expanded to include the entire marketplace startup ecosystem, including investors, founders, executives, lawyers, operators and the vendors and solution providers we rely on.

In 2015, we founded the only conference focused on risk management, trust & safety, compliance and legal strategy for the marketplace startup industry - the Marketplace Risk Management Conference. Since then, we've expanded our scope and gone global with the Sharing Economy Global Summit and much more.

Today, the Marketplace Risk Platform is the most comprehensive source of education, networking and information exchange for marketplace, sharing, gig, peer-to-peer and collaborative economy startups to learn risk management, trust & safety, compliance and legal strategy necessary to successfully launch, grow and exit. From our blog, e-newsletter, Platform Podcast, community app and Live Event Series to our conferences and summits, Marketplace Risk is the first and only dedicated resource for startups to take their businesses to the next level.

Whether you're an investor, founder, executive, lawyer, operator, or one of the vendors or solution providers serving them, we invite you to join us to learn, network and share information to grow the industry together. Learn more about our community by checking out our website at www.marketplacerisk.com.