saifr®

WHITE PAPER

How trust drives the sharing economy

Our new survey confirms safety sells

Overview

Over the past decade, advances in digital technology have created new ways for consumers to purchase goods and services through short-term, peer-to-peer transactions. For example, you can use your mobile phone to order a ride to the airport, spend a week in a vacation house reserved through a home-sharing app, and enjoy takeout delivered directly to your door. All of these sharing-economy or gig-economy purchases are enabled by technology that makes it easy to connect a provider with a consumer.

Both the consumer and service provider take a leap of faith in providing or accepting shared services for or from unfamiliar persons or persons only known through a digital identity.

However, bad actors can use these tech-initiated purchases to defraud consumers. In the example of a home-sharing platform, the third-party contractor could be a trustworthy owner or a scammer attempting to rent property they don't own. They could rent to a responsible customer who is mindful of the property, or they may rent to a customer who damages it.

Inherent in the transaction is a level of risk for the consumer, service/platform provider, and third-party service contractor. The business providing the platform typically carries out some level of due diligence — but not always. Further complicating matters are the ever-evolving local, state, and federal regulations that affect these services. A bad interaction may not only lead to inconsistent experiences for all involved parties; service providers or consumers may also risk property damage, fraud, or worse.

Key terms:

Consumer: A customer who requests a service, such as a delivery or home to rent.

Shared service provider: The organization that runs the app through which the business happens.

Third-party contractor: The person supplying the service, such as delivering items or renting their home.

Trust is an important consideration for consumers when selecting services in this shared economy.

But how important? On behalf of Saifr, research firm MarketSight surveyed 1,000 consumers aged 25 and up across the U.S. in October 2024 to learn how risk, safety, and trust factored into the decision to use sharing- or gig-economy services. This white paper explores the most important data from the survey.

What's inside

saifr

Drivers of consumer engagement

Cost-conscious convenience encourages initial consumer interactions.

Consumers use shared services most frequently for home deliveries and home rentals.

The sharing economy has evolved from peer-to-peer online exchange platforms for swapping goods to a wide array of services consumed through digital platforms. Our survey sought to understand which services consumers use most and how frequently.

When asked which types of shared services they used within the past 12 months — home-sharing, task management, delivery services, or none of those — **57% of surveyed consumers said they've used more than one.**

What respondents use shared services for:

77% for deliveries

56% for home-sharing

29% for task management

Of those who use shared services, a combined 47% say they use these services daily or weekly, with weekly being the most frequent cadence.

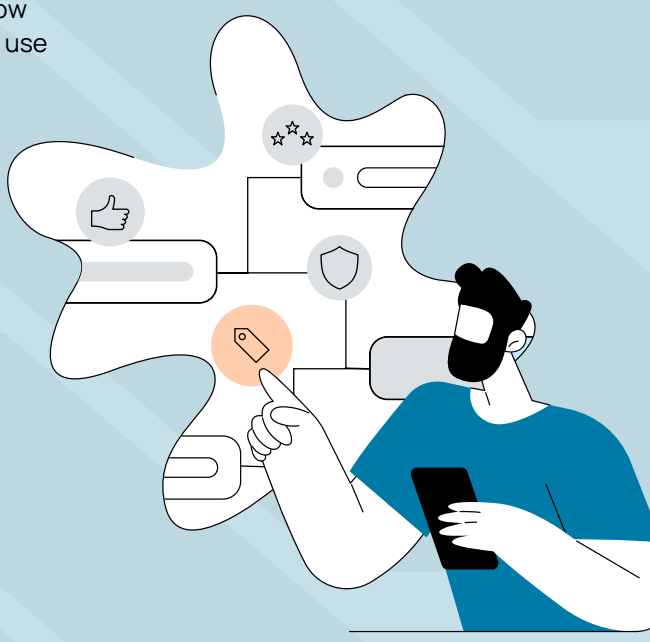
Twenty-four percent (24%) say they use shared-services platforms monthly, and 23% only use the platforms a few times per year. A little less than half (43%) of surveyed consumers said they don't use these services at all.

Cost is **2x to 14x** more important than any other factor when considering shared services.

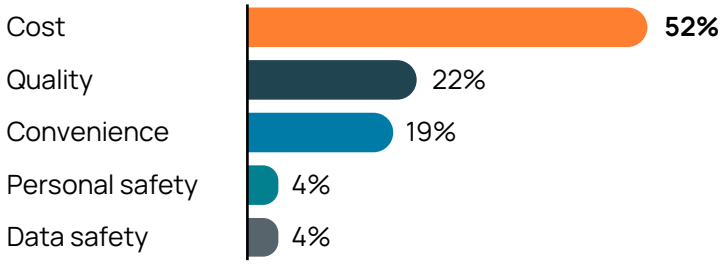
Data also suggest that if costs are too high or the service is poor quality, consumers would not use these services as frequently.

Were consumers selecting these platforms strictly for convenience, and how did cost, quality, and safety influence their choices? When considering the use of sharing economy services, consumers were asked to rank the following factors: cost, convenience, quality, personal safety, and data safety.

Cost was reported to be by far the most important factor considered when using these services, ranking more than twice as important as quality, nearly three times more important than convenience, and about 14 times more important than personal safety or data safety.



Factors that consumers value most:



saifr

Consumer concerns

Fraud, data, and personal safety are top worries when using sharing economy services.

Surveyed consumers said costs were important when considering using a shared service.

But how important are personal safety and data safety when consumers are using the platforms?

The survey dives deeper into consumers' sentiments on perceived safety and risks.

Safety

Consumers were asked to rate how safe they feel when using home-sharing, task management, and delivery services on a scale of one ("very unsafe") to five ("very safe"). Based on the combination of "safe" and "very safe" responses, **consumers said they feel the safest using delivery services.**

74% Deliveries took the top spot, where nearly **three in four** users felt safe

60% Home-sharing services ranked second

43% Task management was last for safety

The shorter the interaction, the lower the perceived risk

Thinking about perceived risks and threats, these responses seem logical. A contractor delivering to a consumer's door is less of a safety concern than a contractor coming inside a home. A correlation also appears between the level of perceived risk and the duration spent engaging in the purchased service.

Potential risks

Consumers were asked to rank their concerns, choosing from the following: personal safety, property damage, theft, data privacy breach, fraudulent charges, poor quality of service, none, or other.

Consumers are considering risks to physical, financial, and digital safety when using shared services. In fact, a service provider's failure in digital security is considered almost as important to users as personal safety.

The weight of these risks underscores why comprehensive strategies to ensure consumer peace of mind are crucial for building consumer trust.

The top three concerns for users of sharing-economy services are, in order:

58% Personal safety

52% Data privacy

52% Fraudulent charges

Trust as a deciding factor

Risk checks and monitoring help screen and secure platforms.

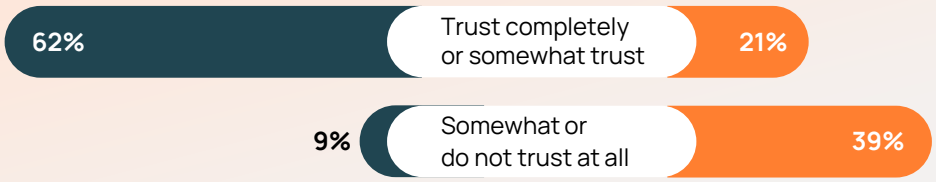
The data show that consumers are weighing safety risks with other factors when considering sharing services. One way shared-services platforms can help consumers feel more secure is to provide transparency around the nature and extent of their risk mitigation programs used to vet contractors. Do they include adverse media screening, background checks, and other methods to help mitigate unknown risks and establish a baseline of trust between a consumer, contractor, and provider? Do they perform continuous monitoring to flag changes? How much do consumers know about these processes, and does knowing make a difference in usage?

Could a lack of trust prevent non-users from becoming service users?

Users | **Non-users**

Trust in the onboarding and monitoring processes

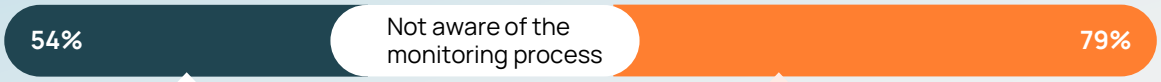
Participants were asked on a scale of one ("don't trust at all") to five ("trust completely"), how much they trust the onboardingand monitoring processes of service providers.



Trust in onboarding and monitoring **is a key factor for non-users**

Awareness of the onboarding and monitoring processes

Consumers were asked if they were aware that most shared-services platform providers conduct one background check during a contractor's onboarding and then annually thereafter.



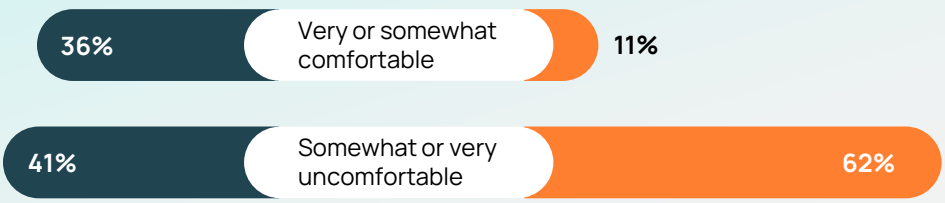
Most respondents did not know providers' onboarding processes may only include one initial background check and then a re-check annually.

Yet, **only 4% of users and non-users believed annual background checks were enough.**

Comfort in giving access to home after passing one background check

Consumers responded on a scale of one ("very unconfortable") to five ("very comfortable") how willing they are to give contractors access to their home or personal space.

20% of users feel very uncomfortable allowing someone who has passed only a single background check into their home.



saifr

Fostering consumer trust

Continuous monitoring could influence certain groups to use services more.

Minimal contractor monitoring could be a potential disincentive to use sharing services.

56% of non-users said monitoring should be continuous

44% of users agreed

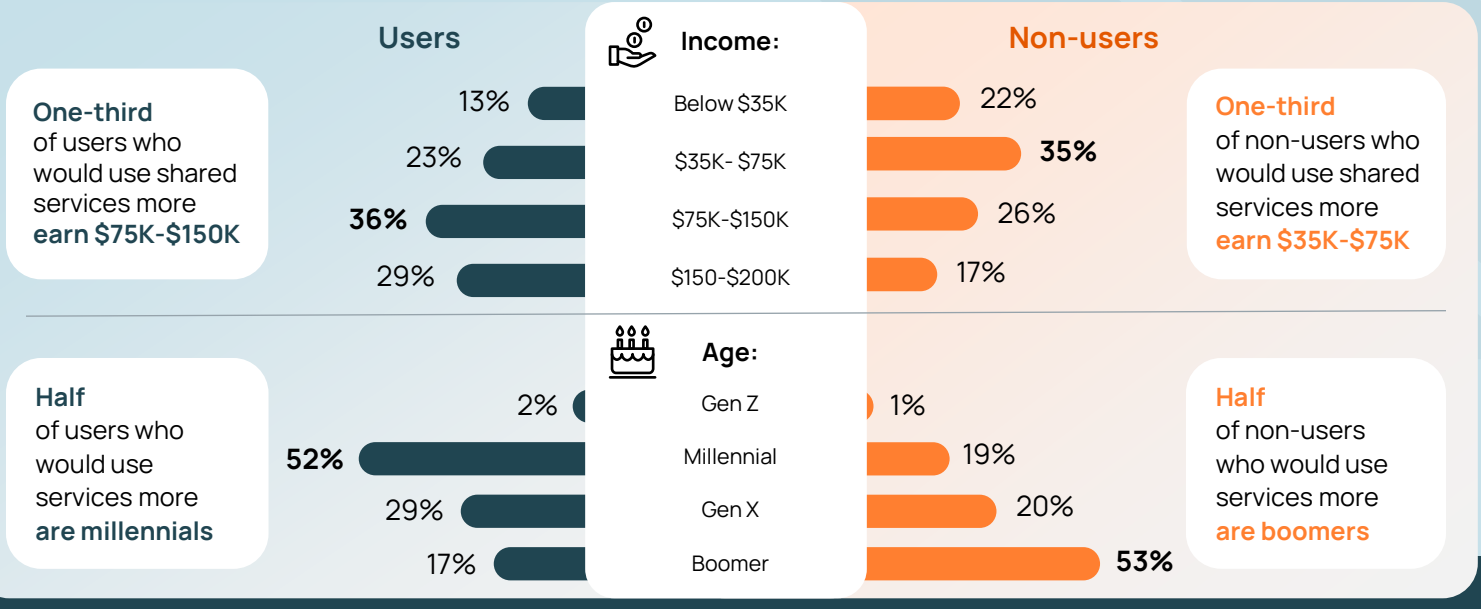
Given that consumers showed concern with infrequent background checks, how often do they expect service providers to monitor their contractors? Very few consumers from both groups believed that annual monitoring (or less) was acceptable.

Enhanced monitoring can help build the trust that drives potential business growth.

58% of **users said they would use shared services more** if they knew providers continuously monitored third-party contractors at little or no additional cost.

29% of **non-users would also use these services** if continuous monitoring were done at little or no additional cost.

A closer look at who would **use shared services more** if monitoring were continuous:



These data show that safety is important to users and non-users.

Both groups think contractors should be monitored continuously, and some consumers from both groups said they would use shared-services platforms more if they knew that the platform providers performed **continuous, real-time monitoring** as a part of their toolkit to help ensure consumer safety.

saifr

Considerations for service providers

Promoting consumer safety can help grow a service provider's market share.

The data show that most people use shared-services platforms, with cost, convenience, and quality being key factors when using services. However, many are also concerned about the safety of these platforms, and their concerns may prevent them from using shared services.

The message is clear: **Consumers want vendors to help ensure their safety.**
To build trust with consumers, shared-services providers should focus on the following areas:

Personal safety

Robust screening measures, including identity verification, background checks, continuous contractor monitoring for potential risks, and safety policies can be effective components of a robust consumer safety strategy to help protect consumers' wellbeing and the service provider's reputation.

Data safety

Service providers that collect sensitive personal and financial information should take steps, such as implementing and auditing data security controls, to help safeguard consumers from identity theft, fraud, and privacy breaches.

Financial safety

Shared services require frequent transactions and use stored payment methods, making secure payment systems, fraud detection mechanisms, and well-defined resolution processes essential to protecting consumers from unauthorized charges.

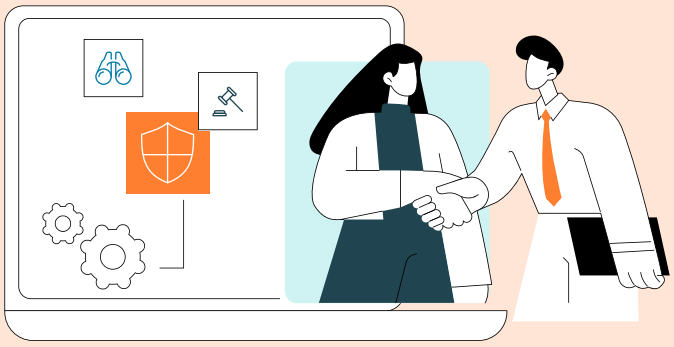
Building trust in an evolving digital marketplace

Consumer safety needs to be a priority for shared service providers that seek to capture new customers and grow their market share with existing customers. Doing so can be a challenge in an evolving digital environment — especially for large platforms managing high volumes of contractors and customers. **For example, it would be nearly impossible to hire enough people to provide continual background screening for all users and service providers on a large platform.** Leveraging additional tools such as continuous monitoring for potential adverse media, watch lists, and other risks, can help augment an overall consumer safety strategy.

Bad actors not only pose a risk for safety but may try to use platforms for illicit activities, such as money laundering through home rental apps. Adding to the complexity is the need to stay compliant with ever-changing local, state, and federal regulations. Unfortunately, one lapse could result in a costly public relations crisis, a lawsuit, and eroded customer trust.

Sharing economy businesses should take advantage of technology to help differentiate their business and foster consumer trust.

They can and should harness emerging technologies like artificial intelligence to support risk mitigation programs, such as continuous monitoring tools that help efficiently detect potential risks among large populations for further investigation by platform providers. Such techniques can help detect potential threats and assist in weeding out bad actors more efficiently.



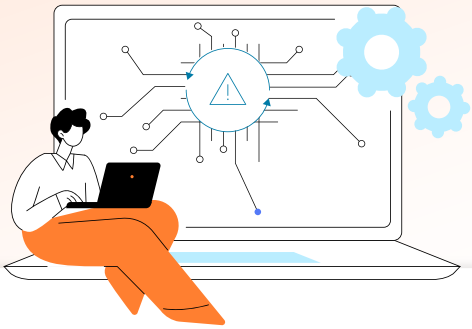
saifr

Screening methods

Enhance trust with SaifrScreen℠.

By incorporating advanced technologies into their operations, sharing economy service providers can create opportunities to build trust with new and existing customers, generating value for their business.

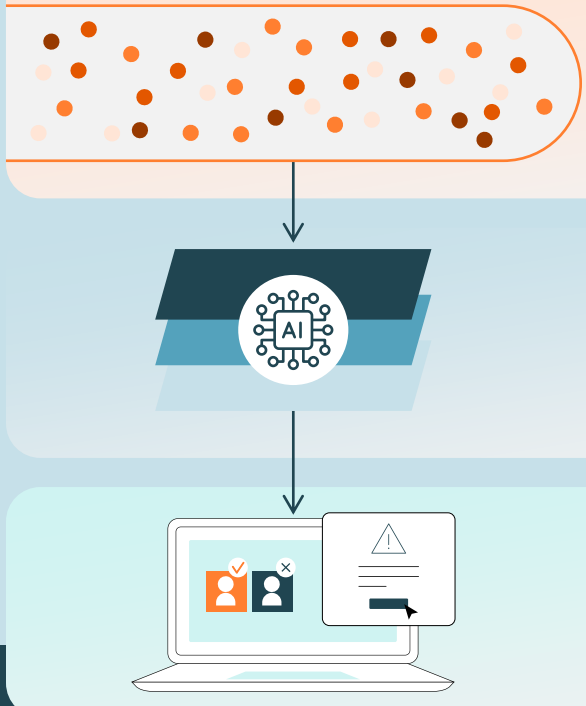
SaifrScreen applies AI to help continuously monitor for potential risks



Integrate SaifrScreen into your processes to:

- Onboard customers and third-party contractors with more confidence
- Maintain ongoing alerts against potential bad actors in your customer and third-party contractor populations
- Get real-time alerts of new or changing potential risks

How SaifrScreen works:



Tap into unstructured data

Provides comprehensive coverage by searching both structured data (sanctions, wanted, and watch lists) and unstructured data (news media, government sources, arrest record aggregators, and/or court record aggregators) to generate leads.

Leverage AI

Uses layers of large language models (LLMs) and natural language processing (NLP) to surface results ranked by relevance and to reduce false positives.

Screen and monitor continuously

Scans entire customer and vendor populations 24/7 against data indexed from 23B webpages (across 190 countries in 160 languages) providing alerts for further investigation as soon as an entity is associated with potential wrongdoing.

SaifrScreen more accurately identifies potential bad actors sooner, helping firms protect their customers, partners, investors, and businesses.

Learn more:
https://saifr.ai/saifrscreen

saifr

About Saifr

Saifr, a RegTech within Fidelity Investments' innovation incubator, Fidelity Labs, is committed to safeguarding organizations from pervasive AI and regulatory risks. Using intelligent technology that efficiently and effectively navigates complex compliance and regulatory requirements, Saifr helps clients save time, reduce costs, and improve accuracy while protecting their firm. Our advanced, AI-powered risk prevention and management solutions include capabilities for marketing compliance review, adverse media screening and monitoring, and electronic communications surveillance. Learn more at https://saifr.ai.

1184478.1.0