FraudShare

For Internal Use Only

Product Overview

FraudShare® is a cost-effective information sharing platform built by our members for the industry to combat account takeover (ATO) fraud perpetrated by unknown and unrelated third party imposters. With over 50 companies using FraudShare it's one of the more widely used fraud prevention tools in our industry.

FraudShare participation not only demonstrates that companies care about protecting their customers, it shows the industry cares about protecting all customers.

LIMRA and Verisk have joined forces to enhance data, analytics, and technology capabilities to build more potent weapons against fraud.

Additional Resources

FraudShare Web Page

FraudShare Flyer

Financial Crimes Prevention Study

5 Min Demo Video

2022 Mid-Year FraudShare Report to Members

2021 Annual FraudShare Report to Members

Key Features and Benefits

Effective

- Enables the industry to work together
- Help to prevent or detect well over 300 3rd party ATO incidents targeting more than $42M in account values

Efficient

- Distinct data with confirmed or known fraud incidents
- Reduces false positives, saving time and investigative expense
- Easy access to incident and threat data

Additional Features:

- Real time email alerts
- Data can be accessed directly via APIs
- Threat indicator data can be used to scan company systems and flag transactions for investigation
- Incident correlation provides additional threat intelligence that can identify other related incidents
- Benchmarking helps better understand ATO activity and how company's experiences compare to their peers.
- Works well regardless of a company's size and/or investigative or IT resources

Trends

- 20% increase in fraud incidents from 2020 to 2021[1]
- 48% of ATO victims have had their accounts compromised 2-5 times. [2]
- ATO leads directly to brand abandonment: 74% of consumers surveyed say they would engage with another provider if their account was hacked[6]
- In 2022, 64% of ATO attacks involved a company's online customer portal[3]

1. 2021 Annual FraudShare Report to Members.
2. ATO attacks increased 307% between 2019 and 2021/, Help Net Security
3. 2022 FraudShare Mid-Year Report to Members

Pricing

- Tier 1, <$25B assets*, **$12,500**
- Tier 2, $25B-$200B assets, **$20,000**
- Tier 3, >$200B assets, **$35,000**

*Based on assets under management that will be protected by FraudShare.

Non-Profit Pricing

As a non-profit trade association, we offer FraudShare to maximize participation while delivering maximum value

LIMRA
Navigate With Confidence

Ideal Customer

To be a qualified candidate a company must:

- Administer accounts containing cash values that may be accessed by fraudsters
- Have at least one individual responsible for ATO fraud investigation and/or fraud prevention
- Ideally have had some previous ATO fraud incidents

Ideal candidates for demos and discussions are those responsible for:

- Investigating 3rd party ATO fraud
- Third party ATO fraud prevention programs
- Leading or working in their company's special investigation unit (SIU), compliance department, or fraud operations team and occasionally a company's cybersecurity team

Customer Pain Points

- Protecting the assets of the enterprise; minimizing financial liability
- Protecting brand and customers' assets
- Minimizing friction with customer experience
- Implementing new oversight solutions with ease
- Reputation risk of not being a good custodian of customer information and assets

Overcoming Objections

Manual entry of data into FraudShare
Directly entering data is quick and easy, and can identify additional threat intelligence to aid in investigation.

Not budgeted for
Because we are a trade association the pricing is affordable

Already using another fraud prevention tool
FraudShare provides additional data that can improve the effectiveness of your fraud prevention program and works even better when combined with other tools.

Don't have the internal resources to support it or the IT resources to integrate it
FraudShare is easy to implement, can be tailored, and works well for companies of varying size and/or available resources.

Competitors

While there are other consortia databases available, none exclusively contain data associated with confirmed 3rd party ATO attacks.

FS-ISAC and NCFTA: their data is broadly sourced and is generally used by a company's info security team and is used to combat cybersecurity incidents.

Evadata ACT: This is specific to our industry. They do not contain threat indicators (e.g. email addresses, phone numbers, etc).

FAQ

Can customers try it out with a pilot?
No, due to the nature of the data and the agreements involved.

Can a company just access the data without providing data?
No, this is a "give to get system."**Can my third party administer (TPA) or BPO provider access FraudShare on my behalf?**
Yes, there are specific TPA\BPO security access roles available.

How many users can access FraudShare?
The standard package allows for 30 users.

Are there different levels of user access?
Yes, each company can assign administrator, full user, and read only roles.

Does FraudShare contain any customer or account information?
FraudShare only contains data related to the incident and the fraudster.

LIMRA
Navigate With Confidence