

Highlights From the 2022 ANNUAL FRAUDSHARE® REPORT TO MEMBERS



ON THE FRONT LINES

Fraudsters are more sophisticated, better organized, and have a greater impact on the financial services industry than ever before — putting individual life, individual annuities, and retirement plans under attack.

Increasingly, LIMRA and LOMA member companies and other leaders in the financial services industry are using the FraudShare® platform and related data to identify, defend against, and prevent these incidents.

53

Companies
Actively Using
FraudShare

Since inception, FraudShare has helped detect more than

460

third-party account takeover (ATO) incidents targeting more than

\$143M

in account values

Important Note: if Fraudshare used to maximum potential ~2,750 incidents, targeting ~\$850m in account values, could have been detected.



The average number of incidents reported by a company in 2022 is also up, continuing to favor earlier in the week

Average Incidents	2020	2021	2022
Per Company Per Month	5	6	7
Per Month	128	161	231
Most Popular Incident Day	Monday (17%)	Tuesday (22%)	Monday (20%)
Least Popular Incident Day	Friday (12%)	Friday (16%)	Friday (15%)

Acquiring Targets — Where, When, and How Often

As companies have moved online, so have the fraudsters — favoring banks with a focus on online and/or digital services and capabilities. The five top banks used by fraudster's account for **40%** of ATO incidents.

The percent of incidents targeting customer portals has continued to increase year over year and now represents **58.7%** of ATO incidents. It's increasingly important that companies have appropriate controls are in place, given the extreme vulnerability. Fraudsters are successfully accessing customer portals in **68.1%** of their attempts, and it takes an average of **8.9** days to detect these attacks.

THIRD-PARTY ACCOUNT TAKEOVER FRAUD

Volume — On the Rise and Here to Stay

During 2022, third-party ATO attacks were up **37%** over the prior year with **2,776** ATO incidents attempting to withdraw over **\$72 million** from **\$678 million** in account values. While ATO attacks increased substantially, the rate at which fraudsters were able to access an account decreased slightly compared to 2021. During 2022, fraudsters succeeded in accessing an account in about **59%** of attempts compared to a **62%** access rate in 2021.

Transactions Attempted	Percent of Incidents Occurred		
	2020	2021	2022
Account Inquiry	25.1%	21.8%	32.9%
Online Registration or Change	20.7%	29.0%	32.2%

In what may be a related finding, there's also been a significant increase in account inquiries. Using the online portals, fraudsters are attempting to register unregistered online accounts and update previously registered accounts.

It's also noteworthy that, while attacks on customer portals increased, those on advisor portals, which had seen a significant uptick between 2020 (0.8%) and 2021 (1.9%), dropped to 0.9% in 2022.

Follow the Money — Disbursements

Financial market fluctuations appear to explain the surge in total account values targeted from 2020 (\$336.7 million) to 2021 (\$752.3 million), followed by a notable decrease in 2022 (\$678.3 million). While it's known that some fraudsters target higher account balances, findings show that most are opportunistic, attacking when they have sufficient data.

Electronic funds transfer (EFT) is the runaway favorite disbursement method overall; however, wire transfer and "other" methods are favored for larger disbursement amounts.



2022 Disbursement Method Analysis

Method	# Requested	% Requests	Average \$ Requests
EFT	615	61.4%	\$66,162
Check	122	12.2%	\$79,474
Wire	90	9%	\$189,836
Other	175	17.5%	\$190,736

Taking Action — Putting "Tech" in Detection

The customer continues to be the number one detector of ATO fraud, identifying about **29%** of attacks, up from 27% in 2021. However, the use of technology is increasing — with about **25%** of attacks detected using a third-party utility designed to detect or prevent fraud.



On average, incidents were detected in about

8.1 Days in 2022

Detection Methods	Percent of Incidents Detected		
	2020	2021	2022
Customer	23.4%	26.8%	28.6%
Third-Party Utility	22.2%	20.4%	25.3%
Employee	31.9%	24.7%	23.6%
Internal Report	12.3%	23.0%	18.0%
FraudShare	3.8%	6.0%	8.1%
Advisor	8.6%	5.9%	5.2%
Other	3.7%	3.7%	2.7%

This is a significant trend since third-party utilities detect incidents at the fastest rate, about

5.4 Days on average

FRAUDSHARE

High Marks — Used Effectively

Companies using FraudShare effectively to monitor their transactions are detecting an average of **20%** of fraudulent incidents. In fact, some are detecting up to **44%** with FraudShare. Notably, 10 of the top 15 FraudShare adopters use its application programming interfaces (APIs).

Top 15 Companies Detecting Most Incidents Using FraudShare in 2022

Average % Detected Using FraudShare

20%

Largest % Detected Using FraudShare

44%



To learn more about Fraudshare and how it can help prevent ATO fraud, visit limra.com/FraudShare.

Note: The above data and analysis were made possible by all FraudShare contributing member companies.

©2023, LL Global, Inc.
0249-2023 (50700-10-730-10007)