

# Highlights From the 2021 ANNUAL FRAUDSHARE® REPORT TO MEMBERS



## FraudShare Continues to Grow

FraudShare is one of the most widely used tools by our members to prevent third party account takeover (ATO) fraud. FraudShare is a resource of related data to help the industry better understand and defend against these attacks.

# 52

Companies  
Actively  
Using  
FraudShare

To date, FraudShare has helped detect over **192** 3rd Party ATO incidents targeting **\$31M** in account values



Average number of monthly incidents by members

**20%**  
from 5 to 6  
per month



## Third Party Account Takeover Fraud Is on the Rise and Here to Stay

ATO fraud continues to increase and evolve. While fraudsters tend to favor the beginning of the week to attack, there doesn't appear to be a particular ATO "season." Fraudsters are opportunistic and strike when they have the data and opportunity.

Both the average account values targeted and the average amounts requested increased over 2020. When it comes to disbursement methods by the fraudsters, EFT remains the top choice and is requested 64% of the time, with check a distant second at 16%. The bank/financial institutions most favored by fraudsters continue to be those known for their online and digital capabilities.

	2020	2021	% Change
Average Account Values Targeted	\$216k	\$280k	30%
Average Fraudulent Disbursements Requested	\$58k	\$80k	38%

## Companies Are Taking Action

Companies relied more on the use of internally developed reporting and analysis capabilities to detect incidents in 2021 — up 83% compared to third party utilities, which were used to detect 9% fewer incidents as a percent of detected incidents.

An important component of any successful fraud prevention program is the integrated use of consortium data. Companies who use FraudShare APIs detect more fraud. FraudShare APIs identified an average of 6 incidents, compared to the 4 detected by FraudShare for those who don't use the APIs.

Efforts to train and equip employees to spot the red flags do pay off as FraudShare data shows employees tend to detect incidents quicker than most other methods — in about 7 days, on average.

Employees detect third party fraud incidents in about

**7  
Days**



## Increasing Online Capabilities Increases Fraud Risk

Data shows large increases in incidents utilizing the customer/advisor portals while attacks targeting contact centers and back-office processing centers decreased. While online attacks were on the rise in 2021 the good news is the percent of incidents in which the fraudster was able to successfully access the account via the customer portal decreased by 16%.

Successful access to accounts via the customer portal decreased by

**16%**



Advisor Impersonations

**Up 92%**



Attacks Utilizing Advisor Portal

**Up 156%**

## Attacks Involving Advisors Are Trending Up

While very low, the percent of incidents involving advisor impersonations and accessing advisor portals increased substantially in 2021. Since attacks impersonating an advisor/using the advisor portal can provide fraudsters greater access to customer accounts, it's important for companies to focus on ensuring the requisite controls are in place.

## Email Compromise Schemes Are on the Rise

The increases in customer and business email compromise schemes is likely related to the increase of online and email fraud schemes perpetrated against the general public over the past couple of years. As a result of all these schemes there are significant amounts of personal data including emails and cell phone data available to fraudsters. Email and cell phone data is especially helpful for fraudsters who wish to open online accounts or takeover online accounts that rely on the customer's email or cell phone as an authenticator.

Business Email Compromise Schemes

**Up 119%**



Customer Email Compromise Schemes

**Up 47%**



## Take Action to Help Prevent Fraud

It remains critically important to focus on regularly evaluating and enhancing your online security access and authentication controls, especially those associated with your advisors.

In an environment where online and mobile capabilities are increasing, it will be practically impossible to defend against fraudulent attacks without utilizing technology to its fullest, whether it be internally developed tools, third party utilities, and/or consortium data such as FraudShare.

[Click to enlarge](#)

To learn more about Fraudshare and how it can help prevent ATO fraud, visit [limra.com/FraudShare](https://limra.com/FraudShare).