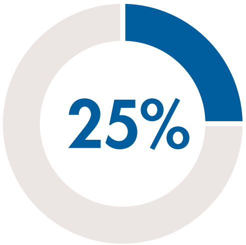
FraudShare

2023 Midyear Report to Members

January 1, 2023 — June 30, 2023

Average Fraudulent Disbursement Requested

$157,258



of incidents were detected by **customers** within **10.2** days on average

The average number of days it took to detect an ATO Incident

6.3

Average account value targeted by fraudsters for 2023

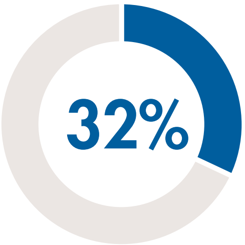
$312,457

Third-Party Account Takeover Incident Analysis

Third-party account takeover (ATO) incidents are up 25 percent over last year, as of June 30, 2023. Consistent with the last few years, fraudsters continue to be most active on Mondays and Tuesdays, slowing down towards the end of the week, with companies experiencing the fewest attacks on Fridays. For the first half of 2023, FraudShare is seeing an average of 241 incidents occurring per month — an increase over last year's 231 incidents per month. This represents a 4 percent increase over last year and a 49 percent increase over 2021, where the average number of incidents submitted monthly was 161. Over the last few years, the average number of incidents submitted by company per month has been trending upward. For the first half of 2023, this number has climbed to eight incidents per company per month.

Average Incidents	2020	2021	2022	2023 YTD
Per Company Per Month	5	6	7	8
Per Month	128	161	231	241
Most Popular Incident Date	Monday (17%)	Tuesday (22%)	Monday (20%)	Monday (22%)
Least Popular Incident Date	Friday (12%)	Friday (16%)	Friday (15%)	Friday (15%)

Navigate With Confidence



of incidents target the **contact center** and take **4.8** days on average to detect

5 banks are associated with **39%** of All ATO Incidents

Detection Methods, Access Rate, and Timing

Over the last three years, customers were the number one detection method for identifying third-party ATOs; however, a new detection method has stolen the number one spot for the first half of 2023 and that is third-party utility. Our Members continue to extract threat indicators from FraudShare and load the data into third-party tools such as Pindrop, Nuance, SPLUNK and GIACT to help identify suspicious activity in real time. Eight of the top 15 FraudShare users actively connect to FraudShare's API to help eliminate manual entry into their detection tools and processes. Companies also report that the average number of days to detect these incidents is 2.9 days, which is significantly less when compared that to the number two detection method, the customer, which takes 10.2 days on average to detect.

Top Detection Methods	Percent of Incidents Detected				% Accessed	Avg. Days to Detect
	2020	2021	2022	2023 YTD		
3rd Party Utility	22%	20%	25%	28%	46.7%	2.9
Customer	23%	27%	29%	25%	81.3%	10.2
Employee	32%	25%	24%	22%	51.9%	4.9
Internal Report	12%	23%	18%	15%	69.3%	5.6

When Used Proactively, FraudShare Helps Detect Third-Party Account Takeovers

Top Companies that Detected Most Incidents Using FraudShare YTD 2023	
Average % Detected Using FraudShare	30%
Largest % Detected Using FraudShare	73%

Companies that proactively use FraudShare and have detected at least one (1) incident are detecting an average of 30 percent of their incidents using FraudShare. Additionally, 61 percent of these companies utilize FraudShare APIs to regularly ingest and use FraudShare data to detect suspicious activity.

EFT remains the number **1** disbursement method used by fraudsters; average amount requested is

$122,265

Access Points, Access Rates & Timing

Fraudsters continue to target customer portals and contact centers most often. Companies reported that the customer portals were targeted 912 times in the first half of 2023. During those attacks, the fraudsters were able to access the customer's account 71.9 percent of the time. Unfortunately, when the fraudster's target customer portals, the average number of days it takes an organization to detect these incidents is 6.8 days. With fraudsters now able to beat multi-factor authentication and one-time passcodes on an increasing basis, we anticipate these numbers to increase even further in the future.

Access Point	Percent of Incidents Detected				% Accessed	Avg. Days to Detect
	2020	2021	2022	2023 YTD		
Customer Portal	45.4%	55.8%	58.7%	62.9%	71.9%	6.8
Contact Center	48.0%	39.3%	35.7%	31.7%	49.5%	4.8
Processing Center	12.2%	9.1%	7.7%	8.8%	82.8%	9.7
Advisor	3.2%	2.5%	3.0%	3.1%	31.1%	3.9
Advisor Portal	0.8%	1.9%	0.9%	1.5%	63.6%	17.0

Fraudulent Transactions Attempted

Fraudulent disbursement transaction attempts have increased sharply during the first six months of 2023. So far, 34.3 percent of all the incidents attempted in 2023 involve a disbursement request, a 20 percent increase over 2022. Consistent with the sizable increase in fraudulent disbursement requests is the considerable increase in the average balances targeted and average amount requested (see Disbursements below). Online registration and online credential changes remain firmly in second place and represent a significant percentage of all fraudulent transactions requested.

Transactions Attempted	Percent of Incidents Detected			
	2020	2021	2022	2023 YTD
Disbursement	34.5%	27.8%	28.5%	34.3%
Online Registration or Change	20.7%	29.0%	32.2%	33.7%
Account Inquiry	25.1%	21.8%	32.9%	31.2%
Bank Account Change	21.8%	19.1%	23.5%	23.2%
Phone Change	11.2%	10.3%	15.1%	15.5%
Email Change	8.2%	9.6%	12.2%	13.4%
Address Change	4.5%	4.8%	3.2%	2.9%
Account Opening	1.6%	3.9%	5.9%	2.5%

Note: Multiple transactions can be associated with an incident (% won't equal 100%).

Monday is the most popular day for an attack

22% occur on Mondays, **15%** occur on Fridays

Disbursements

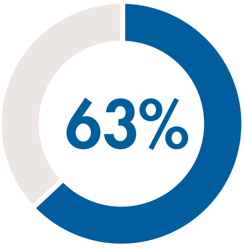
For the first half of 2023, both the average account balance targeted and the average amount requested have increased significantly. The average account balance pursed in 2023 is 31 percent larger than the amount targeted in 2022, and the amount requested was 88 percent larger than the amount requested last year. So far during 2023, there have been 72 incidents that targeted accounts with balances exceeding $1,000,000 and 79 incidents involving disbursement requests exceeding $100,000.

Account Value & Disbursements	2020	2021	2022	2023 YTD
Total Account Value Targeted	$336,669,851	$752,353,351	$678,301,903	$453,062,554
Average Account Value Targeted	$227,551	$352,596	$238,418	$312,457
Total Disbursement Requested	$33,309,363	$108,392,763	$72,363,256	$79,887,307
Average Disbursement Requested	$58,131	$182,479	$83,463	$157,258

Fraudsters continue to favor the use of EFTs for disbursement requests, which accounts for almost 56.7 percent of all disbursements requested. While wire requests are less prevalent, they tend to be for much larger amounts on average. It is interesting to note that while fraudulent disbursements via checks are infrequent, they are often for large amounts, $103,362 on average.

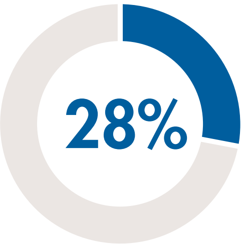
2023 Disbursement Method Analysis

Disbursement Method	# Requested	% Requested	Avg. $ Requested
EFT	345	56.7%	$122,265
Other	157	25.8%	$15,868
Wire	67	11.0%	$322,316
Check	50	8.2%	$103,362



of attacks targeted the **customer portal** and were detected within **6.8** days on average

Third-party ATO incidents up **25%** during first half of 2023



28% of incidents were detected by **third-party utilities** within **2.9** days on average

Banking Trends

Following last year's trends, five banks account for 39 percent of all incidents in which banking information was provided, and fraudsters continue to exploit smaller regional banks to launder fraudulently obtained funds. The most popular bank continues to be Sutton Bank with its nine brick and mortar locations in Northern Ohio. Coastal Community Bank is another small regional institution with 14 branches in the North West corner of Washington State that has become popular with the fraudsters. Metabank, Green Dot, and Go2bank continue to be the most often used banks with strong online and digital presences commonly used by the fraudsters.

Top Five Banks Used in 2023 YTD

Top Five Banks Used 2023 YTD	Routing #	# of Incidents	% of Incidents*	# of Companies	Account Values	Total Fraudulent
Sutton Bank	041215663	68	11%	14	$21,404,769	$927,507
Metabank (Pathward)	073972181	57	9%	19	$24,337,789	$1,043,794
Green Dot (Bonneville Bank)	124303120	57	9%	10	$14,001,644	$959,608
Go2bank	124303162	35	6%	14	$6,064,103	$469,080
Coastal Community Bank	125109019	33	4%	11	$1,932,123	$406,416

*Represents the % of incidents in which banking information was provided.

Companies most effectively using FraudShare detect an average of **30%** of their incidents using FraudShare

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

0974-2023 62105-10-730