

Operationalizing the ID Network® Member Fraud Attributes – A Case Example

Number of Instances	1		2–5		6+	
	Firing Rate	Fraud Index*	Firing Rate	Fraud Index*	Firing Rate	Fraud Index*
Times Fraud Reported at Address in Last 6 Months	0.18%	9.06	0.02%	37.38	0.01%	2.95
Times Fraud Reported at Address in Last 12 Months	0.34%	6.23	0.04%	26.21	0.02%	8.89
Times Fraud Reported at Address in Last 24 Months	0.59%	4.40	0.12%	13.72	0.03%	8.39
Times Fraud Reported at Home Phone in Last 6 Months	0.30%	41.37	0.11%	24.01	0.01%	▶ 47.42
Times Fraud Reported at Home Phone in Last 12 Months	0.48%	26.32	0.15%	19.72	0.04%	10.77
Times Fraud Reported at Home Phone in Last 24 Months	0.72%	18.08	0.19%	16.39	0.10%	5.04
Times Fraud Reported with SSN in Last 6 Months	0.15%	84.96	0.01%	5.20	0.00%	-
Times Fraud Reported with SSN in Last 12 Months	0.28%	47.37	0.01%	218.18	0.00%	-
Times Fraud Reported with SSN in Last 24 Months	0.40%	33.68	0.03%	111.53	0.00%	-
Times Fraud Reported with Name & DOB in Last 6 Months	0.09%	137.09	0.00%	-	0.00%	-
Times Fraud Reported w/ Name & DOB in Last 12 Months	0.14%	88.58	0.00%	221.20	0.00%	-
Times Fraud Reported w/ Name & DOB in Last 24 Months	0.21%	59.98	0.01%	98.47	0.00%	-
Times Applied with Home Phone in Last 1 Day	2.19%	9.98	0.04%	204.86	0.00%	-
Times Applied with Home Phone in Last 5 Days	3.25%	7.63	0.17%	75.71	0.00%	-
Times Applied with Home Phone in Last 15 Days	▶ 5.52%	5.60	0.67%	27.81	0.01%	626.77
Times Applied with Home Phone in Last 30 Days	9.49%	3.62	1.96%	13.49	0.08%	154.08
Times Applied with Work Phone in Last 1 Day	0.44%	1.98	0.05%	2.30	0.00%	-
Times Applied with Work Phone in Last 5 Days	0.64%	2.29	0.11%	3.79	0.00%	-
Times Applied with Work Phone in Last 15 Days	0.96%	2.68	0.31%	3.70	0.02%	3.18
Times Applied with Work Phone in Last 30 Days	1.11%	3.00	0.48%	3.75	0.10%	5.07
Times Applied with SSN in Last 1 Day	1.15%	16.78	0.02%	296.19	0.01%	4.15
Times Applied with SSN in Last 5 Days	1.92%	12.15	0.10%	91.61	0.01%	20.39
Times Applied with SSN in Last 15 Days	3.81%	7.76	0.42%	35.15	0.02%	110.74
Times Applied with SSN in Last 30 Days	7.36%	4.95	1.42%	14.92	0.05%	102.24
Times Applied with Name & DOB in Last 1 Day	1.37%	8.63	0.01%	291.64	0.00%	-
Times Applied with Name & DOB in Last 5 Days	1.42%	9.56	0.02%	209.80	0.00%	-
Times Applied with Name & DOB in Last 15 Days	1.48%	11.05	0.02%	285.04	0.00%	-
Times Applied with Name & DOB in Last 30 Days	1.55%	10.98	0.03%	245.03	0.00%	-
Times Applied with Address in Last 1 Day	1.02%	7.65	0.02%	137.76	0.01%	35.68
Times Applied with Address in Last 5 Days	1.89%	5.29	0.13%	34.62	0.01%	82.95
Times Applied with Address in Last 15 Days	3.77%	3.76	0.50%	15.26	0.02%	103.06
Times Applied with Address in Last 30 Days	6.49%	2.56	1.40%	8.17	0.05%	92.84
SSN is Invalid	0.00%	-	n/a	n/a	n/a	n/a
SSN is Frivolous	0.01%	2.75	n/a	n/a	n/a	n/a
SSN Issued before DOB	0.81%	1.78	n/a	n/a	n/a	n/a
SSN Reported as Deceased	0.11%	2.41	n/a	n/a	n/a	n/a

▶ In this example, 5.52% of identity events are likely to have at least one other application for credit within the last 15 days using the same home phone number.

▶ If you receive an identity event that has six or more frauds reported at the home phone in the last 6 months, the fraud rate is 47 times higher than average.

■ Gray shaded rows indicate applicant may be the victim or the perpetrator of identity fraud. This may impact the chosen investigative techniques.

■ Red shaded cells indicate applications that have a fraud attribute with a fraud index of seven or higher.

* Fraud Index is the multiple of the average fraud rate.
 – A dash represents no occurrences of this scenario in the sample population.

Use Case Example 1

ABC Company is a medium-sized ID Network Member. Before becoming an ID Network Member, ABC did not have an effective process to prevent identity fraud. Today, ABC sends a batch file of all new applications to ID Analytics each night. Because they do not have an existing relationship with the new applicants, they need to screen applicants for identity fraud to protect their organization.

Each morning ABC receives back from ID Analytics the fraud attributes on the prior day's applicants. ABC's fraud manager reviews any applications that have a fraud attribute with a fraud index of seven or higher (shaded red in the preceding chart). ABC's fraud manager chose a fraud index of five to begin reviewing applications to balance controlling fraud risk with the cost and resources available for investigation.

ABC has also built custom rules that queue for review any events where certain combinations of attributes have fired, such as "Times Applied with Home Phone in Last 15 Days" and "Times Applied with Address in Last 15 Days", even when individually they may not meet the five times the average fraud rate threshold. A high velocity of applications within a relatively short timeframe is a condition that the ABC Company fraud manager wants to investigate further.

This process enables ABC to effectively prioritize events for fraud review. Because ABC chooses to send new identity events overnight in a batch, they continue to conditionally book new accounts, then once they receive the ID Network Membership fraud attributes, high-risk accounts are suspended pending further fraud investigation.

Understanding which attributes, such as the "Times Applied by SSN" attributes are likely to be triggered by events initiated by identity fraud victims (rows shaded in gray in the preceding chart) helps ABC apply the right investigative techniques to protect themselves from fraud while also protecting their relationships with customers or prospects that have been victimized by identity fraud.

Use Case Example 2

DEF Company is a small-sized ID Network Member with fewer than 500,000 customers. In addition to using their ID Network Membership to screen new customers for identity fraud, they also send any changes to the identity elements of current customers through a similar process.

For example, each night they send ID Analytics any address changes received from customers that day. The next morning, ID Analytics sends back the fraud attributes associated with those identity events. DEF's fraud manager reviews any events that come back with a fraud attribute with a fraud index of seven or higher. DEF's fraud manager chose a fraud index of seven to review identity changes for existing customers to balance the trade-off between reducing fraud risk and managing the positive customer experience that DEF strives for with its customers.

Like ABC Company, DEF has also implemented some decision rules that evaluate combinations of attributes to queue customer identity changes for review. This helps DEF protect their customers from account take-over and enhance their Red Flag compliance programs.