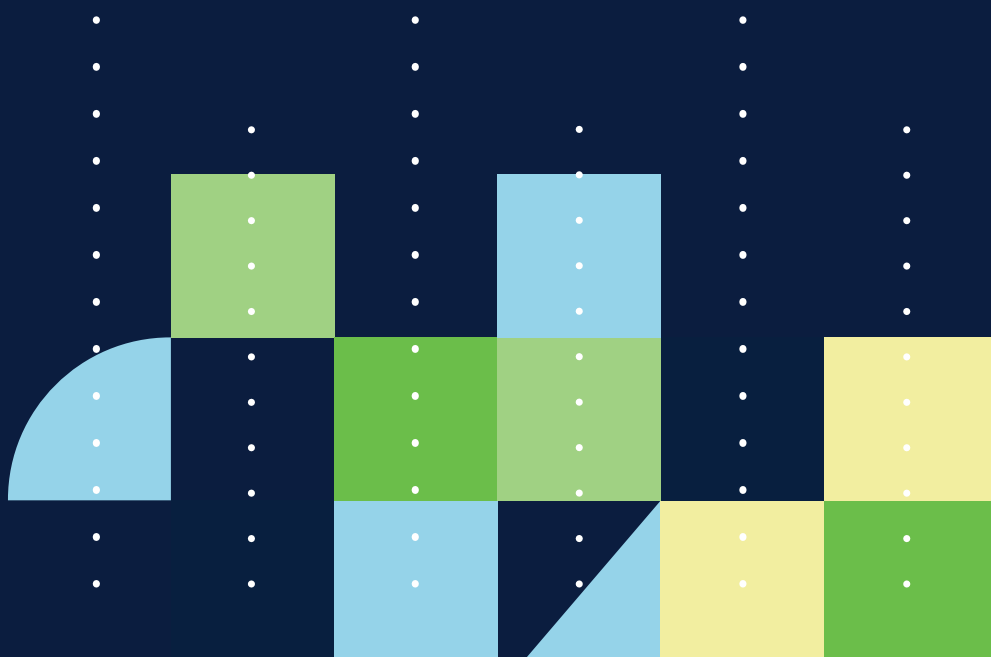
DATAVISOR

Leading U.S. Credit Card Issuer Uses DataVisor's Machine Learning Solution to Reduce Application Fraud Losses



Leading U.S. Credit Card Issuer Uses DataVisor's Machine Learning Solution to Reduce Application Fraud Losses

CHALLENGES

- Third-party and synthetic fraud were causing large financial losses
- Unnecessary reviews resulting from false positives were delaying legitimate applications
- Large alert volumes and high manual review rates were increasing operational costs for fraud teams

SOLUTIONS

- Proactively captured coordinated and unknown fraud by identifying patterns across applications and enabling faster model iteration
- Empowered the organization to create a frictionless experience for good customers by lowering the number of false positives
- Boosted operational efficiencies by enabling bulk decisions for the entire fraud ring

RESULTS

additional fraud captured

detection accuracy

0.17%

good user false positives

>$15M

fraud losses and operational savings in USD

ABOUT THE CLIENT

DataVisor recently partnered with a top U.S. credit card issuer to deliver an effective and scalable solution to fight application fraud. This organization offers a variety of credit products to help their customers finance goods and services purchases, and it processes over 20 million applications every year. Still, the client was challenged by rapidly-increasing and unpredictable waves of coordinated fraud attacks across their online channels.

CLIENT CHALLENGES

Capture Coordinated Third-Party and Synthetic Fraud

The client was experiencing an increase in application fraud, but their existing tools were not up to the challenge of withstanding coordinated attacks that included hundreds of applications sharing similar patterns. The attacks were sophisticated, and featured a range of complex approaches. The fraudsters used stolen identities (third party fraud), often resulting from data breaches, as well as synthetic identities, and additionally, they recruited people to open new accounts.

Because the organization did not have a systematic way of finding links between different fraud incidents, and was unable to detect coordinated attacks in real time, they continued to fall prey to fraudsters' efforts. A more sophisticated solution was needed; one that could surface tell-tale patterns from the traces fraudsters invariably leave behind, despite their efforts to avoid detection.

Reactive Fraud Detection and Slow Model Iteration

Prior to successfully implementing DataVisor's solutions for fraud detection, the client was relying on rule-based systems and multiple supervised machine learning (SML) models. These approaches were unable to capture new and constantly changing patterns.

The rules were reactive and required frequent updates while the SML models were dependent on labeled training data that was perennially slow in arriving. Refreshing a supervised machine learning model was taking the client 6 to 12 months, and consistently accurate detection still remained a problem. It was clear that a proactive solution was the only way the client could stay ahead of the fraudsters.

Balance Risk with Customer Experience

The client was looking to manage risk while simultaneously keeping customer experience intact and free of unnecessary delay. For each genuine customer reported as suspicious, it was taking the client anywhere from several hours to two weeks to open a case, perform manual reviews, and take action to verify the applications. These delays were creating unnecessary friction and turning away good customers.

Additionally, their operational costs were increasing due to large volumes of alerts and high false positive rates. Their operational team was overwhelmed by alerts that required intensive manual reviews and there was a critical need for a solution that significantly reduced the time needed to manage their work efficiently.

HOW DATAVISOR HELPED

Immediate ROI and High Accuracy with DataVisor's Unsupervised Machine Learning Solution

DataVisor's client needed to minimize losses from unknown and coordinated attacks. They needed to improve operational efficiency without negatively impacting the customer experience, and reduce time-consuming and costly manual reviews. The DataVisor solution was able to meet all these objectives.

The client was able to fully integrate the DataVisor solution within a matter of weeks without the need for pre-existing fraud labels, historical data, or an extensive training period. They began to see results right away, as the new system was immediately able to detect fraud that had bypassed their existing solutions, and provide real-time scores that were highly accurate. DataVisor also enabled faster model iteration within days for agile detection.

DataVisor's powerful unsupervised machine learning (UML) solution found hidden connections between seemingly isolated incidents, and identified new attack patterns that revealed highly sophisticated fraud attacks. DataVisor's solution takes a holistic approach to reviewing applications by analyzing profile information, cross-account linkages, behavioral data, and digital footprints such as device IDs, datacenter IP subnets, email addresses, and browsers.

By performing trend and pattern analysis, DataVisor's machine learning model captured 25% more fraud beyond what the existing systems were able to detect — saving the card issuer more than 15 million USD in a single year. The solution also caught fraudsters early in the application process—usually two days to a week earlier than other solutions — thus avoiding costly manual reviews and providing further savings to the client.

Enhanced Operational Efficiency and Confident Decision-Making

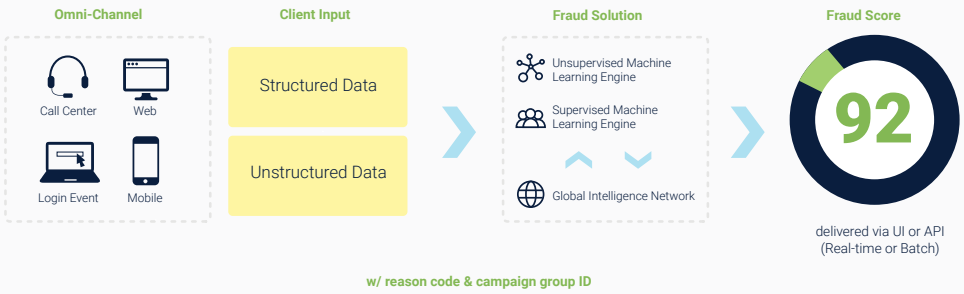
By working with DataVisor, the client's operational team was able to significantly improve efficiency. DataVisor's systems were able to discover clusters of linked accounts, and then group those results. Subsequently, analysts only needed to review a handful of sample cases before confidently making bulk decisions that would apply to all of the applications within the same fraud ring.

The results were dramatic—94% detection accuracy and a false positive rate of only 0.17%. The client developed high confidence in DataVisor's results, and was able to pursue aggressive customer acquisition strategies without the worry of heightened fraud risk.

Over the long term, the client expects to extend DataVisor's machine learning solution to other products—both consumer and small business.

HOW DATAVISOR DETECTION WORKS

The DataVisor approach enables proactive fraud protection. While conventional rules or model-based solutions require "pre-knowledge" of how attacks work to be effective, DataVisor's systems are architected to detect fraud attacks without any historic labels, large datasets, or training time. Drawing on a proprietary UML engine, DataVisor's solutions accelerate detection by analyzing all accounts and events simultaneously and identifying suspicious clusters of malicious activity—even at the point of account registration. This approach is ideal for finding new and unknown attacks because it does not require historical data and constant retuning.



To enhance detection efforts and enrich decision-making, DataVisor also leverages its Global Intelligence Network (GIN), which is comprised of anonymized non-PII data from over 4 billion protected accounts and 800 billion events across the globe. The GIN contains rich information on digital data such as IP address subnets, prefixes, proxies and data centers, user agent strings, device types and OS, email address domains, and more. Information from the GIN feeds into machine learning algorithms to further improve overall detection.

FRAUD RINGS DETECTED

Fast-Evolving Fraud Ring

A fraud ring consisting of over 400 applications quickly changed patterns in two weeks. Despite this level of sophistication, DataVisor's systems were able to surface the fraudulent activities.

		Same card	Two distinct Incomes	Different IPs but from the same data center	All QQ.COM email domain from China	Old iPhone OS 9 and Xiaomi MI5	Same browser
	NAME	CARD	INCOME	IP ADDRESS	EMAIL	DEVICES	BROWSER
WEEK 1	Jon S	Card A	133k	107.160.**.244	JSY12343**@QQ.COM	iPhone 5s OS 9	Chrome
	Daenerys T	Card A	145k	107.160.**.23	ZHAN2344**@QQ.COM	Xiaomi MI5	Chrome
	Arya S	Card A	133k	107.160.**.4	WANG894**@QQ.COM	iPhone 5 OS 9	Chrome
	Tyrion L	Card A	145k	107.160.**.84	FAN234**@QQ.COM	iPhone 5 OS 9	Chrome
	Cersei L	Card A	145k	107.160.**.143	CHEN634**@QQ.COM	Xiaomi MI5	Chrome
	Theon G	Card A	133k	107.160.**.97	XIAO545**@QQ.COM	Xiaomi MI5	Chrome
Fraud Pattern Changed		Target Another card	Different incomes	IPs changed but still from the same data center	Email patterns changed	Still the same device, OS and browser	
	NAME	CARD	INCOME	IP ADDRESS	EMAIL	DEVICES	BROWSER
WEEK 2	Sansa S	Card B	133k	107.160.**.35	SAN**@MSN.COM	iPhone 5s OS 9	Chrome
	Jaime L	Card B	145k	107.160.**.47	JAI**@MSN.COM	Xiaomi MI5	Chrome
	Jorah M	Card B	133k	107.160.**.221	JOR**@MSN.COM	iPhone 5 OS 9	Chrome
	Khal D	Card B	145k	107.160.**.232	KHA**@MSN.COM	iPhone 5 OS 9	Chrome
	Samwell T	Card B	145k	107.160.**.55	SAM**@MSN.COM	Xiaomi MI5	Chrome
	Robb S	Card B	133k	107.160.**.18	ROB**@MSN.COM	Xiaomi MI5	Chrome

The email patterns and application information was easy to change, but the device fingerprints were too expensive to be diversified completely.

* Data shown above is representative and is not from actual customer data

Evasion Techniques

The fraudsters obtained stolen identities or created fake synthetic identities to apply for credit cards. They changed patterns very quickly to bypass the detection of rule-based engines and supervised machine learning models.

Patterns DataVisor Detected

The group of fraudsters applied for Card A using QQ.com email domains from China. Their devices were old iPhones (OS 9) and Xiaomi MI5s. After a one-week break, the same group applied for a different product, Card B, by changing names, incomes, and email domains. However, their IP addresses were still from the same data center and their device types, and the OS and browsers, remained unchanged. DataVisor was able to detect these two waves of fraud ring activity by correctly spotting the common pattern of behavior.

Third-Party Fraud Ring

DataVisor identified a fast-growing third-party fraud ring that submitted more than 2700 applications in just two weeks.

Names and email addresses are not correlated

126.com domain is from China but the addresses are in U.S.

Different cards

Different incomes

Different IPs but from the same data center

NAME	EMAIL	ADDRESS	CARD	INCOME	IP ADDRESS	DATAVISOR SCORE
Jon S	ZHOU12**@126.COM	34** Sa** Blvd, CA	Card A	133k	50.51.***.69	93%
Daenerys T	WANG23**@126.COM	22** Mi** Ave, CA	Card B	123k	50.51. ***.202	93%
Arya S	CHEN34**@126.COM	68** Vi** Dr, CA	Card A	103k	50.51. ***129	93%
Tyrion L	HUA15**@126.COM	43** Mi** Ave, TX	Card B	113k	50.51. ***.19	93%
Cersei L	MO87**@126.COM	36** He** Dr, TX	Card A	93k	50.51. ***.4	93%
Theon G	DAI65**@126.COM	12** Co** Road, TX	Card B	153k	50.51. ***.23	93%
Sansa S	ZHAO90**@126.COM	56** Sh** St, NJ	Card A	128k	50.51. ***.224	93%
Jaime L	QIN55**@126.COM	75** St** Blvd, NJ	Card C	139k	50.51. ***.202	93%

Fraudsters used real people's names and addresses in the U.S. But their email addresses were from 126.com – a China exclusive domain, and their emails and names are not correlated.

*Data shown above is representative and is not from actual customer data

Evasion Techniques

The "applicants" presented seemingly excellent creditworthiness and diverse demographic information—with names and addresses matching those of real people in the U.S.—but all the other information was fabricated. They used datacenter IPs to hide true locations.

Patterns DataVisor Detected

All applicants were from the U.S. but their email domains were 126.com—a China-exclusive domain—and their names and email addresses were not correlated. Most applicants had the same IP prefix and their IPs were from a single data center in Los Angeles.

CONTACT US

If you are interested in learning how DataVisor can help bring your fraud detection to the next level or wish to start a trial to assess your current fraud exposure level, please contact us at: **info@datavisor.com** or visit us at **www.datavisor.com**

DATAVISOR

967 N. Shoreline Blvd.
Mountain View | CA 94043