FRAUD CASE STUDIES:

Financial Firms Fight Back

DATAVISOR

Introduction

Customers are shifting to digital channels and expect a seamless experience in all of their financial transactions without sacrificing the security of their data. Financial institutions want to provide this frictionless experience. However, financial institutions struggle to balance customer experience with fraud management due to Infrastructure challenges and the shift from individual, one-off fraud attacks to rapidly evolving fraud attacks that are coordinated, large scale, and powered by sophisticated attack techniques.

It is no surprise that fraud prevention professionals understand that their current approaches to fraud are proving to be inefficient and ineffective.

In an Aite Group's survey of FIs, FIs mention disparate systems, ineffective solutions and operational overheads as key pain points to be addressed.

(Source: Aite Group)

Customer data is spread out over disparate systems. Financial institutions lack an easy way to gain a holistic insight into fraudulent activities, and many banks continue to rely on individual case-based reviews at a huge operational cost. Traditional approaches that include rules-based detection and even machine learning approaches that are reactive rely on historic loss labels and frequent training. Moreover, many solutions that rely on anomaly-based detection lead to increased false positives and customer friction.

Unfortunately, a lot of information that financial institutions use to verify user identities is readily available online because of data breaches and social engineering. It's becoming easier for fraudsters to create synthetic identities using authentic information to initiate account takeovers, loan fraud, and even money laundering.

It doesn't have to be that way. A comprehensive suite of solutions that is purpose-built to create data intelligence for fraud detection can help FIs to be more proactive and stop fraud before it happens. DataVisor's transformational solutions helps FIs not only stay ahead of their known fraud patterns but also protects them against new and emerging threats by using a combination of approaches for omnichannel, omni-data protection.

Learn how four key financial services companies are leveraging DataVisor to mitigate their fraud and risk exposure and reduce fraud losses while delivering superior customer experience.

Contents

PAGE NO. 13

Leading Loan Provider Improves Fraud Detection and Customer Experience with AI

- Client Challenges
- DataVisor Solutions
- Client Success with DataVisor

25%
fraud detection uplift

90%
detection accuracy

5x
more efficiency compared with table-view reviewed

PAGE NO. 16

Top Online Payments Platform Uses DataVisor Machine Learning Solution to Stop ATO Attacks

- Client Challenges
- DataVisor Solutions
- Fraud Patterns Detected
- Client Success with DataVisor

45%
increase in ATO detection

0.7%
false positives

CASE STUDY:

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

CLIENT A top U.S. credit card issuer that processes over 20 million applications every year.

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

in fraud losses and operational savings (USD)

CLIENT CHALLENGES

The client was experiencing an increase in application fraud, but its 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, it 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 Iteration Model

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.

Balancing 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, the company's operational costs were increasing due to large volumes of alerts and high false-positive rates. Its 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 the work efficiently.

DATAVISOR SOLUTIONS

The client implemented DataVisor's solution within weeks without the need for pre-existing labels, data sets, and training. The company began to see results immediately and detected fraud that had previously been bypassing its existing solutions. The Unsupervised Machine Learning (UML) platform was able to identify connections between seemingly isolated incidents.

FRAUD PATTERNS DETECTED

After implementing DataVisor, the institution uncovered a number of complex fraud rings and patterns, including the following:

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.

CLIENT SUCCESSES WITH DATAVISOR SOLUTIONS

After implementing DataVisor, the credit card issuer began to see results right away, detecting fraud that had bypassed its previous fraud detection systems immediately. The company was able to proactively capture coordinated and unknown fraud with DataVisor's UML, which looked at holistic data to detect patterns across applications and speed up model iteration.

With DataVisor, the company was able to capture 25% more fraud cases than it had with previous systems, resulting in savings of more than $15 million in just one year.

At the same time, the company was also able to reduce its number of false positives and catch fraudsters earlier in the process. With 94% detection accuracy, the client was able to pursue aggressive customer acquisition strategies, confident in its fraud prevention solution.

CASE STUDY:

Top Financial Institution Uses DataVisor to Fight Fraudulent Transactions in Real-Time

CLIENT A large global financial institution that services over 200 countries and has been in the financial services industry for over 100 years.

CHALLENGES

- Millions of chargebacks from fraudulent transactions continued to slip through existing detection systems.
- Customers were having a negative experience due to high false positives that led to the rejection of valid transactions.

SOLUTIONS

- Use DataVisor machine learning solutions to boost fraudulent transaction detection beyond the company's existing solutions.
- Leverage DataVisor's Global Information Network (GIN) to prevent fraud in real-time to mitigate the impact of financial losses before they occur.

RESULTS

increase in detection

detection accuracy

0.9%
false-positive rate

$12M
annual chargeback savings

CLIENT CHALLENGES

While the organization had existing systems in place to try and detect and deter fraudulent transactions, it was struggling with the increasing sophistication and scale of the attacks that were plaguing its defenses.

Outdated Rules-Based Systems

The organization's supervised machine learning fraud models, which worked incredibly well on training and testing data, were unable to detect new and emerging fraud attacks that were unknown before and during model production.

High Level of Fraud Not Detected

Significant numbers of fraudulent transactions were successfully eluding the client's systems, and fraudsters were making handsome profits in the process. Both the company and its customers were suffering.

Lengthy Response Times

Fraudulent transactions are extremely difficult to catch because the decision to block a transaction needs to occur within seconds. Failure to do so can mean serious financial loss.

Too Many False Positives

Unintentionally rejecting a good user's transaction will negatively impact their experience. This has a downstream effect on the company's top line. The attacks were too numerous, evolved too fast, and were too sophisticated.

DATAVISOR SOLUTIONS

DataVisor's machine learning solution is designed to identify fraud patterns without the use of historic labels, training, or large data sets. A proprietary Unsupervised Machine Learning (UML) engine analyzes all accounts and events to identify suspicious activities in real time, including the point of account registration. In doing so, DataVisor excels at finding both known and unknown attacks.

FRAUD PATTERNS DETECTED

A large fraud ring included 500+ fraudulent accounts that were created to transfer money to different recipients. Relying on DataVisor's fraud solutions, the client was able to detect these accounts in real-time by uncovering telltale patterns.

Different senders	Different sender locations	Different recipients	Same recipient locations	Different sender IPs	Same sender device IDs	Similar money amount
Sender	**Sender Location**	**Recipients**	**Recipient Location**	**Sender IP**	**Device ID**	**Money Amount**
Jon S	San Francisco, CA	Jorah M	Miami, FL	107.160.**.244	798237***4	440
Danny T	Dallas, TX	Jorah M	Miami, FL	57.163.**.23	798237***4	462
Arya S	Seattle, WA	Ned S	Miami, FL	97.150.**.4	798237***4	470
Tyrion L	New York, NY	Ned S	Miami, FL	118.120.**.84	798237***4	453
Cersei L	Las Vegas, NV	Bran S	Miami, FL	207.191.**.143	435674***7	465
Theon G	Orlando, FL	Bran S	Miami, FL	87.6.**.97	435674***7	448
Sansa S	Los Angeles, CA	Joffrey L	Miami, FL	87.130.**.244	435674***7	468

Evasion Techniques

All the sender's accounts had different IP addresses and names and they sent money to different recipients. The seemingly-legitimate attack patterns made it hard for the client's existing solutions to detect them.

Patterns DataVisor Detected

Similar patterns were discovered within the fraud ring–the sender's accounts were all registered from data center IP subnets, and the senders all used the same device IDs to transfer the same amount of currency ($440-$470) to the same locations. DataVisor's contextual detection strategies and holistic data analysis brought these coordinated activities to light.

CLIENT SUCCESSES WITH DATAVISOR SOLUTIONS

DataVisor's proprietary unsupervised machine learning (UML) algorithms detected 20% more fraudulent transactions on top of what the company's existing solutions were able to identify, with 94% accuracy. By capturing new and fast-evolving fraud patterns without the need for historic labels, large datasets, or training time, the impact was immediate and significant—more than $12M in savings.

The organization was able to prevent more than 90% of fraudulent transactions and make real-time decisions with confidence. This, in turn, allowed the client to improve overall customer experience by preventing good customers from being rejected.

CASE STUDY:

Leading Loan Provider Improves Fraud Detection and Customer Experience with AI

CLIENT A subprime lender offering short-term and intermediate-term loans with 900+ retail locations throughout the United States.

CHALLENGES

- The company needed strong controls when vetting applications, especially applications received online, due to the high risk of financial loss resulting from immediate approval of fraudulent applications.
- When combating fraud, the firm wanted to avoid alienating its good customers and eliminating friction when approving valid loan applications.
- The firm needed to understand emerging fraud patterns and attack types in order to take proactive action against evolving threats.

SOLUTIONS

- Establish fraud detection and prevention systems that scale as the company grows.
- Leverage unsupervised machine learning as a layer of fraud defense to prevent fraud in real-time.
- Layer fraud prevention methods so that criminals can't reverse engineer fraud detection techniques.
- Use knowledge graph to visualize linkages among correlated accounts and uncover hidden fraud patterns.

RESULTS

fraud detection uplift

systematized fraud detection methods with accuracy

5x

more efficiency compared with table-view reviewed

CLIENT CHALLENGES

The client is a subprime lending firm with hundreds of retail locations across the country. The company specializes in helping people get quick access to capital to handle life's little challenges, from needing a little breathing room until payday to making surprise repairs on their car.

First and foremost, the company prides itself on a customer-centric experience. But as fraud continues to rise across the U.S., the firm found that current fraud prevention techniques weren't allowing it to expeditiously serve its customers to its internal standards.

As a result, the firm encountered the following challenges:

Poor User Experience

The firm wants to make acquiring a loan as easy and frictionless as possible. As a whole, the company is weighted more toward customer experience than it is toward fraud deterrence, but it also acknowledges that it can't simply allow fraud to happen if it wants to remain profitable. In response, the company believes that segmenting customers based on their level of risk can help to reduce the potential for fraud.

Rule-Based Systems

The company lacked reliable, consistent measures to detect and prevent fraud. The controls that were in place were standard rule-based fraud detection, which lacked a well-organized approach. As the company began to grow, it realized its current fraud prevention measures didn't scale and support its growth.

Fraud Models Required Constant Retuning

The firm relied on population-based fraud models to detect people that were most likely to commit fraud. Anyone who didn't fall into this model and committed fraud was able to easily fly under the radar. These models required constant updating for the most accurate representation, which was time-consuming and costly to do.

Lack of Accurate Anomaly Detection

When anomalies to the fraud model were detected, it usually resulted in a large number of false positives. In return, this created additional friction for good customers, who may end up seeking loans from a competitor in the future.

DATAVISOR SOLUTIONS

The lender took a multi-layered approach to fight fraud, including the use of DataVisor's unsupervised machine learning. UML looks at patterns criminals take to uncover coordinated fraud and complex crime rings across different fields that a human wouldn't be able to analyze and connect.

Some of the ways the lender is using DataVisor to protect against fraud include:

Identify Suspicious Patterns Across the Entire Customer Lifecycle

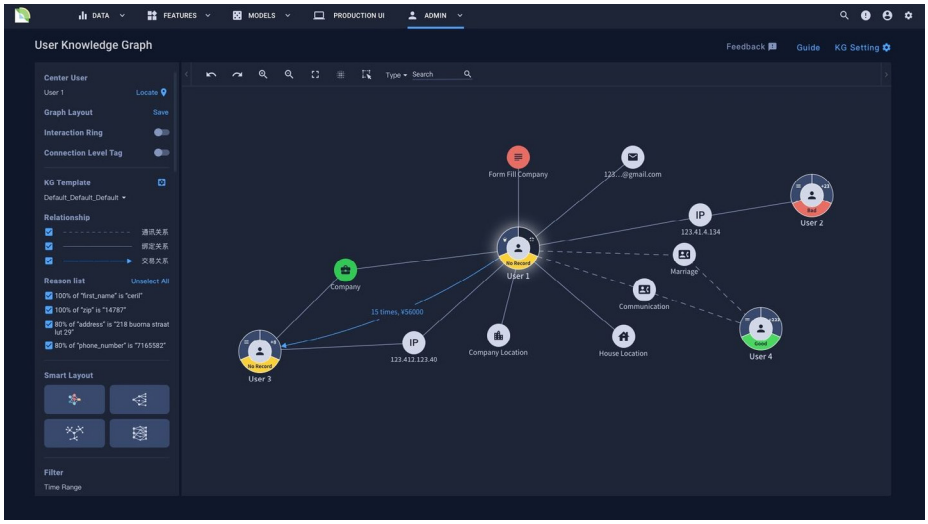
Once a customer is established in its system, DataVisor can track their behaviors throughout their life cycle, even when using more than one retail location. DataVisor makes it easy to see why certain activities have been flagged as suspicious, which makes it easier for agents to conduct their investigations.

Detect and Respond to Fraud in Real-Time

The client now has the ability to not only detect instances of fraud, but also eliminate them in real-time. Its goal is to avoid letting fraud through the front door and allow the firm to remain agile.

Investigate Hidden Linkages Using Knowledge Graph

The client is empowered to investigate suspicious cases 5x faster than table-view analysis and make contextual decisions with DataVisor's linkage analysis solution– Knowledge Graph. The client now has the ability to uncover multi-dimensional connections among entities, groups, money flows, IPs, emails, and other attributes in real time, and stop application fraud with speed and high accuracy.



CLIENT SUCCESSES WITH DATAVISOR SOLUTIONS

The client notes that DataVisor's focus on fewer false positives and ease of use are among the top reasons the company chose DataVisor's UML. The firm continues to benefit from DataVisor's global intelligence (more than 4.2 billion accounts) and the ability to take action at the early stages of fraud to mitigate its impact rather than reacting after fraud has been committed. The high accuracy rate and low false positives have enabled the firm to create the frictionless customer experience that allows it to remain competitive in the market.

CASE STUDY:

Top Online Payments Platform Uses DataVisor Machine Learning Solution to Stop ATO Attacks

CLIENT One of the world's largest online payment platforms that enables users to enjoy wallet-free payments via mobile devices and web apps.

CHALLENGES

- New growth in users and transactions resulted in a greater increase in attempted account takeovers (ATOs).
- Successful takeovers resulted in customer frustration and the leak of personal information.
- Existing ATO detection models were ineffective at capturing fast-changing, large-scale ATO attacks launched by sophisticated fraud rings.
- Fraudsters were launching mass attacks after ATOs.

SOLUTIONS

- Complement existing solutions with DataVisor's Unsupervised Machine Learning (UML) to identify coordinated attacks on a large scale.
- UML views all account activity at once to identify suspicious correlated activity in real-time.

RESULTS

increase in ATO detection

0.7%
false positives

CLIENT CHALLENGES

Business growth is a goal for any company, but when that growth also means an increase in attempted account takeovers, one financial platform knew it needed to step up its fraud detection. Some of the company's challenges in finding a solution included:

Inefficient Internal Systems

To mitigate ATOs, the company turned to a team of engineers to monitor reports of abnormal account activities. The teams were using an internal ATO detection system composed of business rules and supervised machine learning models. However, the ATO detection models in place were ineffective at capturing fast-changing, large-scale ATO attacks launched by sophisticated fraud rings.

Inability to Identify Patterns on a Large Scale

Moreover, fraudsters would launch mass fraud attacks quickly after taking over the accounts, typically within a few days. In doing such attacks, subtle patterns existed in the before-takeover and post-takeover account behaviors. Unfortunately, the ATO detection methods were unable to look across accounts and activities at once to identify these attack patterns.

DATAVISOR SOLUTIONS

DataVisor's UML platform complemented the company's existing solutions to identify ATOs on a broader scale with increased accuracy in real time. This eased the burden on the existing team of engineers that were conducting manual reviews to find abnormal account activities.

They accomplished this through two of DataVisor's unique tools:

- ### Unsupervised Machine Learning

  UML identified coordinated ATO attacks across accounts at high accuracy and large scale. The UML Engine viewed all accounts and their associated activities at once, and then surfaced subtle suspicious correlations in real time.

- ### Global Intelligence Network

  DataVisor also leveraged its Global Intelligence Network (GIN), which is aggregated anonymized non-PII data comprised of over 2 billion accounts and 600 billion events from customers across the globe. The GIN contained rich information about digital fields such as IP addresses, proxies and data centers, user agent strings, device types and OS, email addresses, and more. Information from the GIN fed into the UML Engine to further improve the overall detection.

FRAUD PATTERNS DETECTED

Using DataVisor, the company noticed numerous activities associated with fraud rings, including the following:

- **Similar Post-Takeover Activities**

  DataVisor identified a fraud ring involving 200+ accounts who used botnets to hack accounts with weak passwords. The botnets used IP addresses from the same area as the hacked account holders. The hackers also used knowledge-based authentication questions to circumvent traditional ATO detection techniques.

- **Coordinated Attacks from Cloud Data Center IPs**

  DataVisor detected more than 500 accounts that had been compromised. Their IPs were hidden behind a cloud hosting data center in a particular state.

CLIENT SUCCESSES WITH DATAVISOR SOLUTIONS

Upon implementing DataVisor alongside existing ATO detection methods, the company was able to better identify ATOs and mitigate their impact on the customer.

After adding DataVisor to its fraud detection and prevention strategy, the company increased its ATO detection by 45%. What's more, its false positive rate of just 0.7% allowed the firm to continue serving customers with a positive user experience and maintain a strong brand reputation.

About DataVisor

DataVisor is the world's leading AI-powered Fraud and Risk Platform for enterprises. Using proprietary unsupervised machine learning algorithms, DataVisor restores trust in digital commerce by enabling organizations to proactively detect and act on fast-evolving fraud patterns, and prevent future attacks before they happen. Combining advanced analytics and an intelligence network of more than 4B global user accounts, DataVisor protects against financial and reputational damage across a variety of industries, including financial services, marketplaces, ecommerce, and social platforms.

For more information on DataVisor:

info@datavisor.com

www.datavisor.com

967 N. Shoreline Blvd. | Mountain View | CA 94043

DATAVISOR