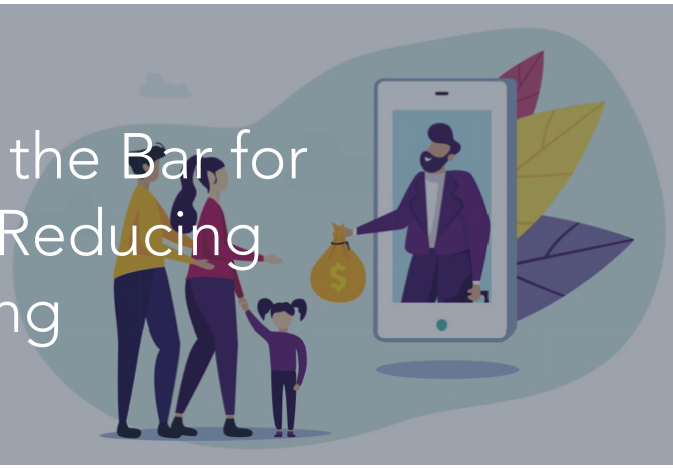
DATAVISOR

BNPL Case Study - Raising the Bar for Customer Experience and Reducing Fraud with Machine Learning



CLIENT

An innovative American financial technology company that pioneered the point of sale finance industry by providing a quick, transparent, and more inclusive lending alternative to consumers.

CHALLENGE

Fraudsters were using synthetic identities to mass register fraudulent new accounts and then requesting loans that were never paid back.

Solving the well-known industry trade-off between customer experience and fraud prevention.

High rates of account takeovers and promotion/benefit abuse indicated that the client had outgrown its insourced fraud model.

SOLUTIONS

- Processed vast amounts of proprietary data with Feature Platform and enriched it with insights from 4.5B third-party accounts and 1T events.
- Leveraged the Rules Engine tool to create and manage commands with heightened efficiency and accuracy.
- Gained a 360° view of fraud data and its connections using DataVisor's Knowledge Graph.
- Leveraged the Case Management toolset to take fast, efficient, and informed decisions in real-time.

RESULTS

41%

reduction in hurt ratio, a measure of false positives.

320+

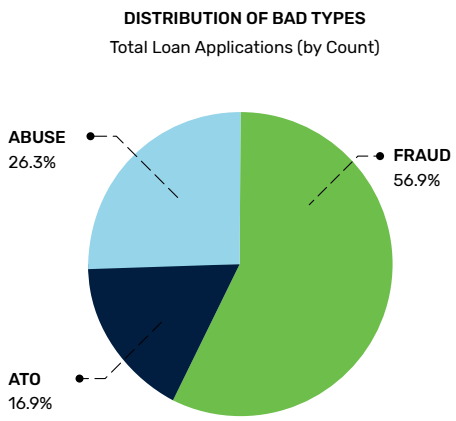
fraud rings detected, some of them related to over $80k in losses per attack.

5x

estimated review efficiency improvement.

CLIENT CHALLENGES

The client was experiencing three different types of fraud, distributed as follows:



In this context it approached DataVisor with the following top-of-mind goals:

- Reducing Friction for Good Borrowers

Reducing the hurt ratio was determined as a top priority because the client expressed that a high-quality customer experience was paramount to success in a highly competitive market.

The hurt ratio measures false positives by indicating how many non-fraudulent events (i.e. credit applications) are flagged for review for every fraudulent one. The client experienced a hurt ratio of five (5/1), which means that its fraud detection system was flagging five good credit applications for review for every fraudulent one. A low hurt ratio means a smoother customer experience where good borrowers are not subject to unnecessary identification measures.

- Increasing the Percent of Fraudulent Applications Detected

A low rate of fraud detection ultimately resulted in first payment defaults, which reduced the client's profits.

- Uncovering Coordinated Fraud Attacks

Since it operates in a highly dynamic environment where thousands of consumers request small to medium-sized loans every day, the client needed a solution that could handle and make sense of vast amounts of data to stop organized cybercriminals.

- Improving Review Efficiency

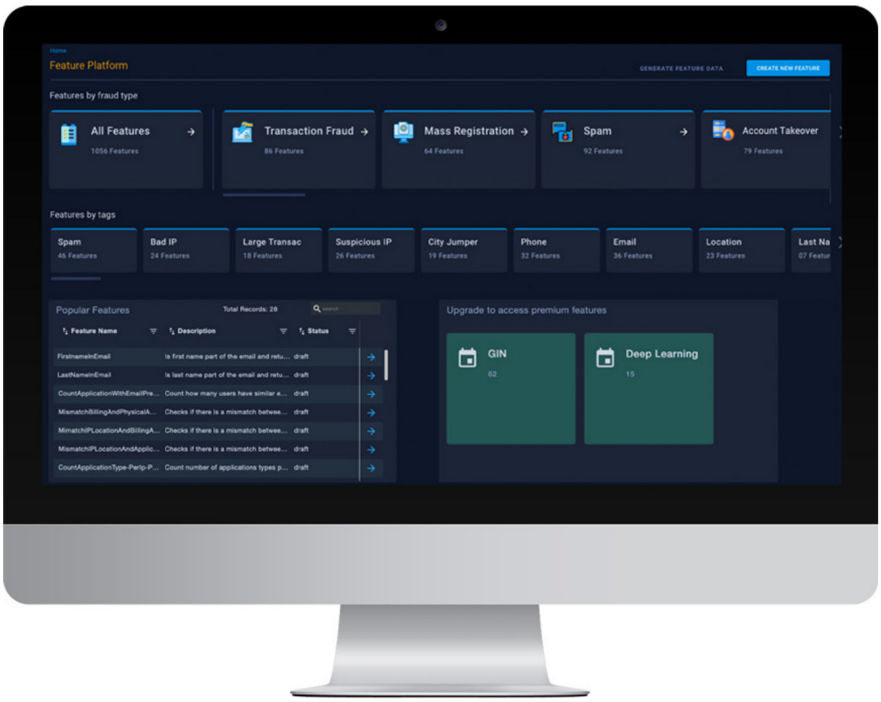
A high review time per application resulted in an increase in operational costs for the client because it had to hire more employees, which reduced the scalability of its business model.

CLIENT SUCCESS WITH DATAVISOR'S SOLUTIONS

FEATURE PLATFORM

The solution starts with data and DataVisor's Feature Platform is the first step. Here, the Client's data was ingested and processed by our cloud-based system and leveraged by the client to automate the feature engineering process and produce thousands of auto-derived multidimensional features. These features are then used to develop artificial intelligence models using DataVisor's unique unsupervised machine learning algorithm as well as open-source machine learning frameworks such as XGBoost.

Led to savings in the tens of thousands of dollars in in-house feature creation costs and machine learning model development and enabled the client to bypass the time-to-market cycle of developing its own features and model, which can last up to five years for comparable financial technology companies.



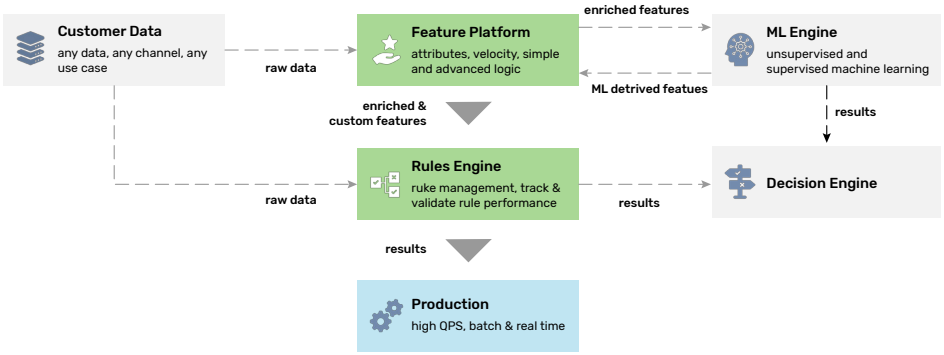
Furthermore, DataVisor's Feature Platform fully integrates with DataVisor's Global Intelligence Network (GIN). It is powered by over 4.1B protected accounts and 800B+ events across industries and it enabled the client to improve its feature derivation and the performance of the model it uses to stop fraud.

> *Improving the customer experience:*
> *More and cleaner data means smarter decisions that thwart fraud but do not flag good users as bad.*

RULES ENGINE

With the data in the right place, the Rules Engine was the next step taken to build a holistic fraud protection approach.

The client leveraged DataVisor's Rules Engine to create and manage command sets and to systematically organize rules and track and validate their performance with advanced capabilities such as backtesting and forward testing. The client also combined the results from the Rules Engine with the results from the machine learning model in a centralized decision-making process that promoted enhanced performance.



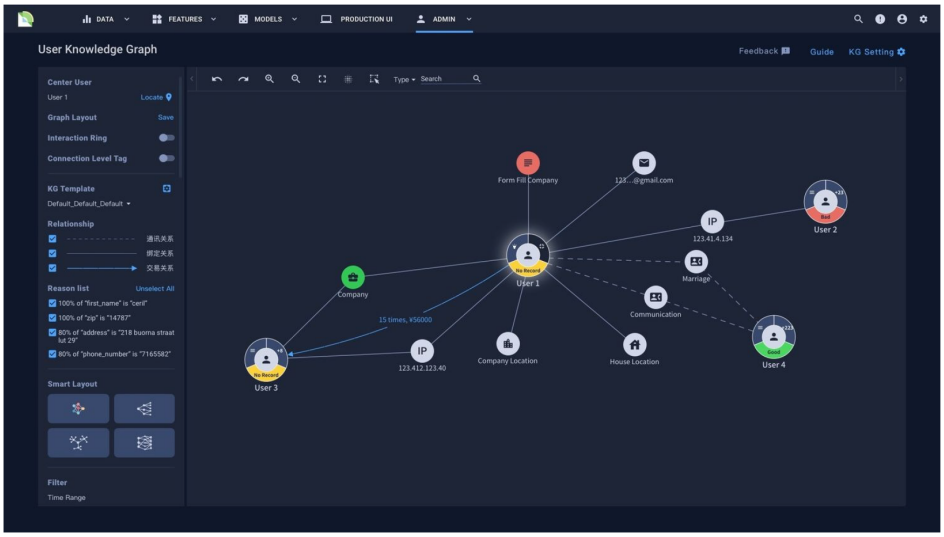
> *Improving the customer experience:*
> *Not all rules are created equal. The client built an auditable and testable rules policy that is in constant self-improvement with the Rules Engine.*

KNOWLEDGE GRAPH AND CASE MANAGEMENT

With a firm base in data and a robust approach to rules in place, the Client began using DataVisor's Knowledge Graph and Case Management tools to visualize fraud insights and take swift actions based on them.

The Knowledge Graph analyzes vast amounts of data to uncover connections between seemingly independent events that are invisible to the naked eye. These connections come in the form of shared entities, groups, money flows, IPs, emails, and other attributes between transactions and are presented in an easy-easy-to-use interface that powers data-driven decisions at the highest level.

Once a comprehensive and interactive view of the data was in place, DataVisor's Case Management tool enabled the client to take context-enriched decisions that stopped fraud with augmented accuracy and an estimated 5x review efficiency gain. Among other features, the client was able to take bulk decisions for groups of events and create custom blacklists and whitelists that simplified internal processes substantially.



A noteworthy feature of DataVisor's solution is the One-Click Investigation, which reduces the amount of friction throughout the customer experience to help operational teams investigate faster and smarter and avoid keeping the customer waiting. Once it builds a linkage, it can automatically connect the new entities or events with previously detected fraud rings; therefore, if the client finds that some new users are strongly connected with known bad actors, the client can immediately mark new users as bad without spending extra time for manual searches or investigations from scratch.

> *Improving the customer experience:*
> *By allowing its team to whitelist good customers and investigate cases with a single click, the client ensured that good borrowers returned and that applications that need review are promptly cleared without keeping the customer waiting.*

LAUNCH AND INTEGRATION

To ensure that the client's needs were addressed promptly and in full, DataVisor implemented its proven deployment strategy. First, a bespoke model that combined the best of supervised and unsupervised machine learning was developed for the client. Then, this model was trained using data from several months' worth of credit applications and their performance. Then, the model was fine-tuned by a consortium of DataVisor engineers and data scientists to enable it to hit the ground running and begin detecting fraud from day one.

DataVisor tested the model and its results were then compared to the observed performance of the loans. Before launch, the client received a presentation that highlighted all the benefits of the DataVisor approach with clear and actionable insights on its own data.

All in all, DataVisor's solution is designed for seamless integration, and its trained team of professionals delivered value to the client within 2 weeks of the start of the process. Adding to this, DataVisor's Knowledge Graph and Case Management tools connect to data from the client's internal systems and third-party vendors in real-time and DataVisor ensured that its solution worked seamlessly with the client's current data architecture, orchestration solutions, and technology stack.

The client only needed to provide its dataset and review the results of the model to get the implementation in motion. From there, the DataVisor team followed a process that has been thoroughly proven across the financial industry.

Comprehensive Fraud Intelligence that Provides Fine-Grained Signals and Risk Scores

- 410 Million+ IP addresses
- 5.3 Million+ User agent strings
- 3.6 Million+ Email domains
- 160,000+ Device types
- 300,000+ OS versions
- 700,000+ Phone prefixes

Insight from 4.1 Billion+ Users and 800 Billion+ Events

- Financial Services
- E-Commerce
- Social Platform
- Mobile & Gaming
- Telecom & Travel
- Insurance

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

Fraud Ring Example #1

charge_ari	time_hour	amount	user_ari	shipping_address	merchant_name	device_id	ipaddress	ipaddress_isp	ipaddress_city	ipaddress_state	charge_state	charge_label
G37K-GJ0W	12/18/20 8:00	869.59	0213-9147-QDUR	d3d6c705901d6efcd1d5d100e434a444e7ab64aa11c1c5b2b815a36cfee82740	[redacted].com	411028409112390000	184.182.16.245	COX COMMUNICATIONS INC.	TUCSON	ARIZONA	incomplete	abuse
ZYSF-113P	12/18/20 21:00	1412				389130771223867000	184.182.16.245	COX COMMUNICATIONS INC.	TUCSON	ARIZONA	captured	abuse
AAIR-1FW0	12/21/20 22:00	759.81				411028409112390000	107.77.229.201	AT&T MOBILITY LLC	CITY OF INDUSTRY	CALIFORNIA	declined	abuse
L66O-Y81Y	12/23/20 16:00	863.38				389130771223867000	107.77.229.47	AT&T MOBILITY LLC	RUNNING SPRINGS	CALIFORNIA	declined	abuse
WH96-97QH	1/15/21 7:00	341.32				411028409112390000	107.77.231.141	AT&T MOBILITY LLC	YORBA LINDA	CALIFORNIA	declined	abuse
Y63L-EBCD	1/17/21 8:00	651.11				411028409112390000	154.16.166.33	GIGENET	CHICAGO	ILLINOIS	declined	abuse
6KK8-674L	1/21/21 5:00	542.41				411028409112390000	184.182.16.245	COX COMMUNICATIONS INC.	TUCSON	ARIZONA	captured	abuse
7SYY-58QV	1/21/21 5:00	455.45				411028409112390000	184.182.16.245	COX COMMUNICATIONS INC.	TUCSON	ARIZONA	canceled	abuse
C8XT-TTK7	1/21/21 5:00	1085.91				411028409112390000	184.182.16.245	COX COMMUNICATIONS INC.	TUCSON	ARIZONA	declined	abuse
C2NR-9Y7F	1/28/21 19:00	1195.69				411028409112390000	184.182.16.245	COX COMMUNICATIONS INC.	TUCSON	ARIZONA	declined	abuse
4BUQ-4TXO	1/29/21 4:00	585.76				225315583538726000	107.77.229.85	AT&T MOBILITY LLC	FONTANA	CALIFORNIA	incomplete	abuse
BU75-3N7R	1/29/21 4:00	1373.75				225315583538726000	107.77.229.85	AT&T MOBILITY LLC	FONTANA	CALIFORNIA	captured	abuse
459W-VO13	1/30/21 0:00	1031.56				225315583538726000	184.182.16.245	COX COMMUNICATIONS INC.	TUCSON	ARIZONA	captured	abuse
2S5B-2Q2E	1/30/21 13:00	1520.71				225315583538726000	184.182.16.245	COX COMMUNICATIONS INC.	TUCSON	ARIZONA	declined	abuse
3K6R-VNT9	1/30/21 13:00	1520.71				225315583538726000	184.182.16.245	COX COMMUNICATIONS INC.	TUCSON	ARIZONA	incomplete	abuse
VHMD-2P8R	1/30/21 19:00	1373.75				225315583538726000	184.182.16.245	COX COMMUNICATIONS INC.	TUCSON	ARIZONA	captured	abuse

The syndicated attack consisted of 112 loan applications over a ~43 day period with a total value of ~$86,204 worth of commodities.

Fraudster has been abusing the payment system and shipping to the same address from [xxxxx.com].

Fraudsters are changing devices to game the system.

Fraudsters switch between IP addresses provide by different ISPs. The IP address can be traced back to locations across the US such as California, Arizona, Illinois, and more.

Out of the 112 applications, 38 applications were not declined and later marked as abuse.

Fraud Ring Example #2

charge_ari	amount	name	user_ari	merchant	shipping_address	device_id	ipaddress	ipaddress_location	charge_state	charge_label
N/A	N/A	4902bf181fa0575a287f832cdfc56562945ab4ec6c5b06c3418ff375bfd333833	2779-8024-KRGL		1d4180bda03c7b99255bb2cb7a6f9dc8ef39fdceba065a23378f6956d3d6dcd4	346861355102269864 (first seen 2020-08-30)	184.89.27.191	MERRITT ISLAND, FLORIDA	N/A	N/A
J6CG-08YN	330			[redacted]	3a164a116613b0b043e025e62d9b000066030b14ae019983050d2f05c457d78c	613747380177109000	24.46.179.225	TORRINGTON, CONNECTICUT	canceled	ato
SD1S-UBSC	330			[redacted]					captured	ato
B7Z6-PKEK	350			[redacted]					captured	ato
HVQU-05PR	340			[redacted]					captured	ato
1D8P-HVFB	350			[redacted]					incomplete	ato
QXFM-X6LS	350			[redacted]					void	ato
XDVY-5JQM	300			[redacted]					void	ato
N/A	N/A	073adb9f181b600a55be7bba64c59aef32d3ec56eaa41df4b6670b7f333cce8c	2923-4699-ODDN		e248f51d0cb4bf6dab654b4b4db2ad74e3e43965da3954f161900a9c34f8915f	385279763988255414 (first seen 2020-07-15)	68.205.112.153	OVIEDO, FLORIDA	N/A	N/A
E9MJ-USF7	283			[redacted]	3a164a116613b0b043e025e62d9b000066030b14ae019983050d2f05c457d78c	613747380177109000	24.46.179.225	TORRINGTON, CONNECTICUT	canceled	ato
14CQ-7TIF	882			[redacted]					incomplete	ato
66E6-XOMY	226			[redacted]					incomplete	ato

The syndicated attack consisted of 50 loan applications with a total value of ~$28,700 worth of commodities.

Two customers with different historical records such as shipping address, device_id, ipaddress, and more are victims of an account takeover attack. Both customers signed up around Jul-Aug 2020.

These commodities ranged from expensive electronics to clothing apparels.

ATO took place on Dec 8, 2020. Fraudster changed the shipping address and the tracked device_id and IP address point to north-west CT.

Out of the 50 loans, 22 applications were not declined, and later marked as ATO.

Fraud Ring Example #3

charge_ari	time_hour	amount	name	user_ari	phone	device_id	email	merchant_name	ipaddress	ipaddress_isp	ip_location	charge_state	charge_label
1GT2-3H6C	12/15/20 22:00	432.53						[redacted]	107.77.231.90	AT&T MOBILITY LLC	[redacted]RIVERSIDE, CALIFORNIA	declined	fraud
RM5L-S05U	12/19/20 11:00	131.76						[redacted]	107.185.245.191	CHARTER COMMUNICATIONS INC	[redacted]RIVERSIDE, CALIFORNIA	captured	fraud
7Q01-JFW3	12/19/20 22:00	523.4						[redacted]	107.77.229.106	AT&T MOBILITY LLC	[redacted]RIVERSIDE, CALIFORNIA	declined	fraud
L1J7-BGOH	12/19/20 22:00	621.9						[redacted] LLC	107.77.229.106	AT&T MOBILITY LLC	[redacted]RIVERSIDE, CALIFORNIA	declined	fraud
TBFT-0K3Y	12/19/20 23:00	481.52	ec2a64cd8915813208bf2a4835bd55717f4324baeccde2e11a2fb6d0730e087	8523-7188-QNJR	fca752cb251476450f87c5ea17511765baacdd46347c4a15497059a53acbb6a3	4879785694790750000	6a35f4ca07a672436925750d7b634cd5dde545fcc7e964c55a371b30b30bab8	[redacted] LLC	107.77.229.106	AT&T MOBILITY LLC	[redacted]RIVERSIDE, CALIFORNIA	captured	fraud
618E-WUAF	12/20/20 4:00	1144.28						[redacted]	107.77.227.69	AT&T MOBILITY LLC	[redacted]RIVERSIDE, CALIFORNIA	incomplete	fraud
GN73-Q0G8	12/20/20 6:00	629.62						[redacted]	107.77.227.69	AT&T MOBILITY LLC	[redacted]RIVERSIDE, CALIFORNIA	declined	fraud
VZR7-ACNY	12/20/20 6:00	629.62						[redacted]	107.77.227.69	AT&T MOBILITY LLC	[redacted]RIVERSIDE, CALIFORNIA	declined	fraud
MATY-04SP	12/20/20 8:00	558.45						[redacted]	107.77.227.69	AT&T MOBILITY LLC	[redacted]RIVERSIDE, CALIFORNIA	captured	fraud
TCER-RN9W	12/23/20 6:00	125.93						[redacted]	107.77.228.95	AT&T MOBILITY LLC	[redacted]RIVERSIDE, CALIFORNIA	declined	fraud

The syndicated attack occurs over a period of 8 days starting from Dec 15, 2020 to Dec 23, 2020. The net amount of the fraud attack is ~$7,035 over 13 transactions

All the loan applications were coming from the same user id with shared PII such as name, phone, device, email.
Fraudsters using one identity for conducting fraud.

Majority of the loan applications (46%) of the fraud ring were targeted at [redacted]

Fraudsters switch IPs within the same IP subnet via different ISPs

Fraudsters are not very matured since they give hint by having IPs from the same location

Out of the 13 loans, 4 applications were not declined, and later marked as fraud.

Fraud Ring Example #4

charge_ari	amount	time_hour	user_ari	name	phone	user_email	merchant_name	ipaddress	ipaddress_location	charge_state	charge_label
77F2-6YA5	678	12/20/20 1:00						None	None	captured	fraud
UCED-J18H	678	12/20/20 1:00						None	None	declined	fraud
SDT0-YS8Q	678	12/20/20 6:00						None	None	canceled	fraud
Y7BK-J29H	678	12/21/20 6:00				89ee51893d57fca6429d368cc71ccd11bdd4ae2c511922a3bb22f912092c33bd	[redacted]Stores	None	None	captured	fraud
FJH4-ES3N	678	12/22/20 1:00						None	None	captured	fraud
CFR5-Y56U	920.51	12/22/20 7:00						None	None	captured	fraud
85XH-C7WW	808.1	12/23/20 5:00	0798-0801-YJZF	01faacb4c9f2e6ce20f73253c858b69ded884716cbab6fe6e09fd4e2b3322996	400f646fc28b88e20cbe70cb3e056a182f0c556676f5bf2f7abd2284be4e39a8			None	None	captured	fraud
0M68-J693	920.51	12/23/20 23:00						174.65.6.144	SAN DIEGO, CALIFORNIA	captured	fraud
DAMG-YVFK	920.51	12/24/20 19:00				d7e6cbafeb8dfc981c697f476fde6a908e23d884106148cee2fe6a6b5fe76ad2		65.74.237.114	LOS ANGELES, CALIFORNIA	declined	fraud
G79V-YI02	920.51	12/24/20 19:00					[redacted]	65.74.237.114	LOS ANGELES, CALIFORNIA	declined	fraud
P8RL-6NLJ	1000	12/24/20 19:00						65.74.237.114	LOS ANGELES, CALIFORNIA	declined	fraud
FGNS-9VRQ	678	12/26/20 3:00					[redacted]com	None	None	declined	fraud

The syndicated attack consisted of 14 loan applications over a 6 day period with a total value of ~$10,840 worth of commodities.

All the loan applications were coming for the same user_ari, name, phone but with two distinct emails

71% of the loan applications were targeted for [redacted]

Fraudsters are using IP addresses based out of southern California.

Out of the 14 applications, 8 applications were not declined and later marked as fraud.