SUCCESS STORY
ATM SECURITY

ORGANIZATION
Top 20 Global Bank

DEPARTMENT
ATM and Digital Banking

FOCUS AREA
Security
Operations

AVAILABLE DATA
- Over 2,000 ATM end points
- 30 days activity window
- 4,000 average daily sessions per ATM
- ATM access logs

BUSINESS CHALLENGES
- Unacceptably high ATM losses
- Inability to identify attack methods behind losses
- Existing technology unable to stop sophisticated, evolving attacks
- Siloed and inconsistent data related to ATM operations
- Increasing number of security breaches

PROJECT GOALS
- Reduce cash theft
- Identify physical and logical security breaches
- Detect and predict operational issues

ROI
Significant benefits realized through improvement in detection/loss mitigation, operational efficiency, and customer service.

- Actionable results within days
- Multiple events found in 4 areas: suspected fraud, operational malfunction, data integrity problems, and potential customer service improvements
- Investigation in hours, not weeks with pinpoint forensic information

THETARAY BENEFITS
- Identified previously unknown security events
- Increased detection accuracy with a low false positive rate
- Ability to analyze large sets of data from different sources simultaneously
- No prior knowledge of event patterns necessary to identify them
- Full detection transparency pinpointing the exact root cause of events

CLEAR. CONFIDENT. ACTION.

Background

A large global bank experienced significant cash loss related to their ATM operations in multiple regions. The bank's existing fraud detection and transaction monitoring solutions along with forensic investigation teams were unable to pinpoint the exact source of loss.

Only through a combination of third-party data and additional publicly available information, the bank was able to identify some of the schemes used in what turned out to be a sophisticated, widespread ATM hacking operation that utilized various attack vectors, from malware, to physical attacks, to insider knowledge of the ATM operations.

As the bank discovered the fraud scheme they came to realize the lack of technology/solution to detect and defend against such schemes. Most solutions available on the market were not up to the task due to their inability to intake and meaningfully process large volumes and varieties data simultaneously, such as financial transactions, system access, device logs, web traffic, communication form ATM to the host, machine data, sensor data, SCADA data.

> "Most solutions available on the market were not up to the task due to their inability to intake and meaningfully process large volumes and varieties data simultaneously..."

> "One of the main challenges the bank faced was a dependency on rules-based monitoring systems that are limited in their ability to identify previously unknown fraud patterns."

Challenge

One of the main challenges the bank faced was a dependency on rules-based monitoring systems that are limited in their ability to identify previously unknown fraud patterns. Additionally, if the attack involves multiple domains of data - e.g. transactions, system logs, host communications, sensors – conventional monitoring systems were unable to analyze activity across domains, due to the volume, variety, and velocity of data.

Goals and Objectives

The goal of this project was to detect abnormal activity on the bank's ATM networks in North America with intent to expand to additional geographies globally. Such activities can potentially include fraudulent transactions, malware attacks, operational issues and abnormal activity that is yet to be known to the bank.

Objective 1: Detect anomalous activities indicative of ATM hacking attacks, physical, logical, cyber security breaches, fraud or operational malfunctions

Objective 2: Identify previously unknown events that could be predictors of emerging threats and opportunities

Objective 3: Reduce monetary losses from ATM fraud

Objective 4: Increase operational efficiency and improve customer service

The project had several KPIs:

KPI 1 **Speed to Value:** Fast installation, data ingestion, and turnaround of output are necessary to allow the bank to quickly research and evaluate the cause and impact of detected anomalies

KPI 2 **Independent Solution:** Ability to work independently of other deployed solutions

KPI 3 **No Domain Expertise:** Ability to produce meaningful results based on pure mathematical analysis, without deep domain expertise, using only unsupervised machine learning algorithms

KPI 4 **Low False Positive Rate:** Produce accurate results for review, limiting the false positive noise to a minimum.

Scope and Data

Project scope included a limited data sample from 2,000+ ATM end points for a 30-day period. Close to 6.5 million ATM access logs and almost 9 million ATM transactions were analyzed to detect abnormal activities which were unknown to the bank at that moment.
Despite limited data dimensions that included only a few sources of data and limited feature richness, the KPIs were successfully achieved.

ThetaRay's recommendation to the customer emphasized the importance of rich data sources with multiple dimensions for an even deeper analysis and improved findings.

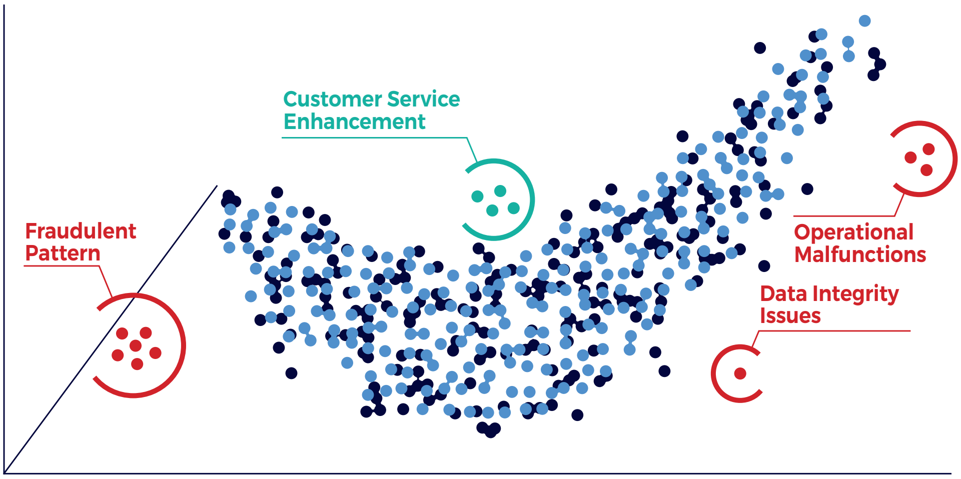
Methodology

ThetaRay's big data analytics platform was implemented on-premise and integrated in the bank's environment. The initial analysis was carried out in less than two-week period and without any data labels or rules. ThetaRay's unsupervised machine learning was able to identify how normal ATM and customer activity looked, so that interesting anomalous events could easily be detected and clustered into meaningful patterns.

Leveraging the clusters, described by representative anomalies, in-depth statistical data surrounding triggering data features, and powerful forensic data analysis capabilities, subject matter experts were able to tell in minutes what clusters reflected interesting events. Many of these events reflected ATM and customer behavior they had not previously been looking for or otherwise anticipated. In addition to the identification of suspicious activities related to fraud, several incremental areas of value surfaced, including improvements in operational efficiency, data integrity, software versioning, and customer service enhancements.

> “ThetaRay's unsupervised machine learning was able to identify how normal ATM and customer activity looked, so that interesting anomalous events could easily be detected and clustered into meaningful patterns.”

ThetaRay Hyper-Dimensional Machine Learning
Learning what's “normal” in multiple dimensions
Identifying threats... and opportunities



RESULT

Findings

ThetaRay was able to process the large volume of historical data in minutes, discover normality and detect meaningful anomalies indicative of fraud. In fact, ThetaRay's hyper-dimensional big data analytics solution increases in accuracy as the complexity and volume of data increases.

Among the findings detected were:

- **Suspected fraud events (new patterns)**
  a. Fraud previously only known to occur in other geographies
  b. Evidence of criminal testing security & fraud controls – multiple withdrawal attempts progressing from high to low amounts
  c. Multiple account information checks followed by withdrawal attempts of $1000 from different accounts
  d. Card skimming and duplication - multiple sessions with same card data used at the same time on different ATMs
- **Previously unknown operational malfunction risks**
- **Previously unknown data integrity issues**
- **Customer service enhancements opportunities**

Sample detected events

Detection 1 – Confirmed Man-in-the-Middle Attack

- Malware deployed on the ATM used to modify messages between the ATM and HOST
- Result: ATM is directed to dispense cash when funds, in fact, are not available in the target account

Detection 2 – Jackpotting

- Fraudsters with insider knowledge of ATM operations hacked into and manipulated its sensors (cassette and door sensors) to enable dispensing small amounts of cash that would not trigger any alerts due to the rounding error pre-programmed in most ATMs.
- Result: the bank lost small amounts repeated hundreds of times across multiple ATMs without triggering a single fraud alert or operational red flag

Detection 3 – Malicious Code Injection Suspected

- Abnormal sessions detected, consisting of dozens of related transactions.
- All withdrawal amounts were consistent small denomination, excluding the first transaction, during a fixed time interval
- Anomaly indicative of programmatic attack

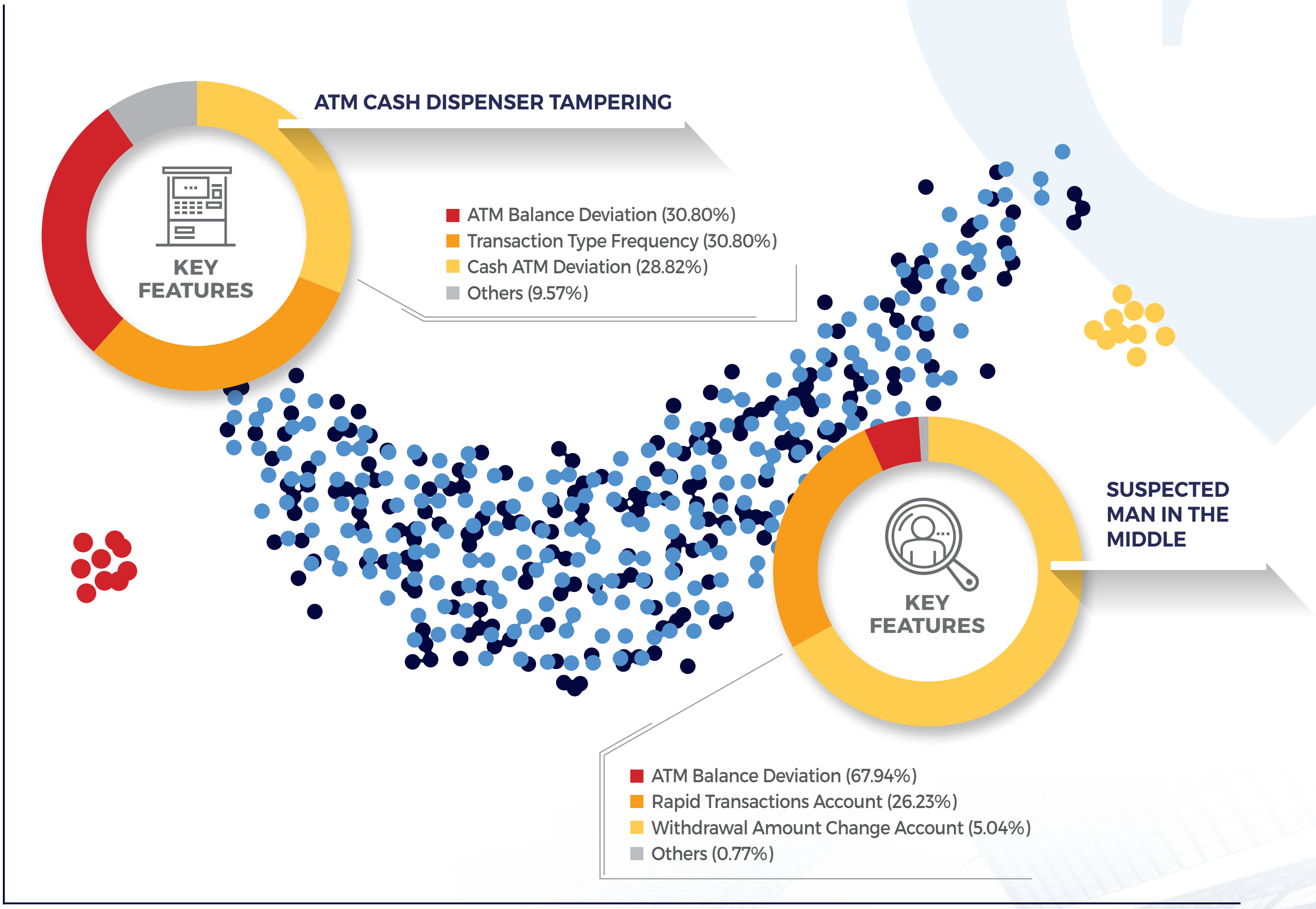
Detection 4 - Operational Issue Detected

- A large cluster of anomalies detected in a single ATM
- Dominant feature triggering the clustered anomalies was a deviation in session length (negative session length). The observed sessions consisted of values in the range of -1 to -109 seconds.
- Anomaly indicative of a data integrity operational malfunction

Detection 5 - Cloned Card Usage Detected

- Abnormal session, suspicious activity indicative of a magnetic copied card and with multiple attempt to check limits on the account.
- Rapid unsuccessful withdrawal attempts (over 30 in 8 minutes) of decreasing amounts until a successful withdrawal is achieved

Sample of detected events



Conclusion

ThetaRay ATM Security is the only advanced AI solution proven to detect evolving fraud perpetrated against individual ATMs and across networks. This gives ATM operators the opportunity to identify and stop fraud losses as quickly as criminals invent new attack methods. While legacy technologies and approaches can help with previously known attacks, this success story shows that gaps in ATM security can be filled successfully today.

Further, ThetaRay has demonstrated the successful ability to identify a variety of events on ATMs that can help organizations reduce maintenance costs and improve customer satisfaction. As shown here, results can begin to surface within days.

While successfully addressing the objectives of the initial deployment phase, this project has already expanded to a global rollout. Early limitations in the breadth of data available constrained the full power of the hyper-dimensional big data analytics, while future phases anticipate increasing success as new data sources become available – driving ever increasing ROI.

> “ThetaRay ATM Security is the only advanced AI solution proven to detect evolving fraud perpetrated against individual ATMs and across networks.”

The ThetaRay Value

ThetaRay’s ATM Security solution built-on advanced AI and unsupervised machine learning arms banks with future-proof tools to detect the most sophisticated and previously unknown ATM fraud before it wreaks havoc. Thanks to sophisticated proprietary processes and mathematical algorithms, ThetaRay has the unique ability to converge multi-domain data, (e.g., ATM machine data, financial transactions, operational logs) and detect ATM threats that have evolved beyond legacy rule-based systems. With ThetaRay, banks and ATM service providers can automatically identify the earliest signs of previously unknown events, irregular ATM operations or malfunctions, and take action to prevent jackpotting, skimming, ATM abuse and rapidly mitigate any negative customer impact.

International Headquarters
8 Hanagar Street
Hod Hasharon, Israel 4501309
Tel: +972-72-274-4999
E-mail: info@thetaray.com

USA Headquarters
462 Broadway
New York, NY 10013
Tel: +1(212) 472-1048
E-mail: info@thetaray.com

THETARAY
thetaray.com