Payment Cards and Risk

How to detect stolen cards, pinpoint suspicious merchants and uncover compromised payment terminals

Gleb Esman | Sr. Project Manager, Anti-Fraud, Splunk
Felipe J. Hernandez | CEO, VPNet, Inc.
September, 2017 | Washington, DC
Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.
Gleb Esman, Bio

1990’s: **Anti-virus research and development:**
Belarus, Israeli anti-virus research and development.

Heuristic virtual machines to detect known and unknown computer viruses and malware.

2000’s-2010’s:
Architecting and software engineering work in space of e-commerce, cryptocurrency, payment processing and digital information management solutions.

Before Splunk, till July, 2015: **Morgan Stanley**.
Working on data analytics solutions for financial services as well as helping to build Splunk-based security and anti-fraud applications.
Leading an effort to leverage Splunk as an anti-fraud platform for online banking.

Since August, 2015 – Sr. Product Manager at **Splunk**, Anti-Fraud Products, San Francisco.

Author of several **Patent Applications for fraud detection with Deep Learning**.
Splunk Platform for Anti-Fraud

Why Splunk is the right fit to address challenges with sophisticated fraud?

▶ Splunk platform acts as the data driven central nervous system of organization.

▶ Splunk aggregates raw data coming in from multiple disparate sources and is indexed in real time.

▶ Data contains traces of anomalous behavior and patterns of suspicious activity.

▶ Advanced analytics and machine learning are utilized to effectively reduce exposure to fraud or loss.
Case: Predicting and Preventing Chargebacks

Leveraging Splunk Machine Learning Toolkit to Predict Chargebacks on Credit Card Transactions
Chargebacks == EVERYONE is UNHAPPY

Intend to protect consumers from unauthorized transactions

- Long - Funds withheld from business until everything clears
- Messy - Chargeback resolution involves lots of paperwork
- Expensive - % processing fee + $10-25+ per case for merchant *regardless*
- Long - Takes 60-90 days to resolve
- Messy - May involve further arbitration between merchant and banks

'I Didn't Buy That': Friendly Fraud Costs Retailers $11.8 Billion a Year

Ecommerce will lose $6.7 billion in 2016 to fraud, according to data from eMarketer and LexisNexis.
Chargebacks Problem

**Merchants** are on the hook to lose

- Payment facilitators recovers chargebacks from merchants
- Issuing bank recovers the funds from the merchant’s bank.
- Merchant bank recovers the funds from the merchant.

**PROBLEM:**

Merchants are kept aside and are notified when it’s too late in the process to prevent penalties, fees and losses of funds and goods.
What Do We Need To Do To Predict Chargebacks?

Large Online Retailer approached Splunk for help

- Need to be able to detect transactions with high probability of chargebacks and put these through extra scrutiny.
- Need to be able to detect that in time close to actual transactions.
- Available data set to learn from was limited to log of 100,000 transactions
- Had confirmed record of only ~100+ confirmed chargebacks
- CC Transactions data contains about ~50 fields describing each transaction
Credit Cards Transaction Data

Some of the available data fields within e-Commerce Transaction logs:

- Date/time
- Transaction Value: $ Amount
- IP Address (+city, zip)
- Customer Email(s)
- Shipping Address(es)
- Billing Address(es)
- **CaseStatus**: Chargeback / Other
- ...

- Customer name
- **Risk Score**
- Customer ID
- Session ID
- Case Status
- Case Extra Data
- Phone number(s)
- ...

© 2017 SPLUNK INC.
Chargebacks: Machine Learning Solution

Splunk Machine Learning Toolkit delivers new SPL commands to apply variety of Machine Learning concepts to your data

https://splunkbase.splunk.com/app/2890/

Machine Learning is an ability of computers to learn and do predictions from data without being explicitly programmed
Building Chargebacks Prediction Model

Leveraging Splunk Machine Learning Toolkit

MLTK Benefits:

- Simple to use. Become data scientist in an hour!
- Web based interface to apply machine learning to your data.
- Guided navigation
- Guided assistants to build models on top of your data without coding skills
  - Predict Numeric and Categorical fields
  - Detect Numeric and Categorical outliers
  - Apply supervised and unsupervised learning techniques to solve problems
  - Detect unknown unknowns to catch attackers and fraudsters
Splunk Machine Learning Toolkit

Single Click interface to access multiple Machine Learning functions
Working with Splunk Machine Learning Toolkit

- Preprocessing steps to scale or normalize data
- Select and configure prediction algorithm
- Prediction results table
- SPL: search to retrieve data
- Show SPL buttons to get ready SPL code snippets
- Confusion matrix: "Quality" of model
Building Chargebacks Prediction Model, cont.

General Steps

1. Devise SPL search to retrieve data
2. Select features available within data that may be useful
3. Consider preprocessing steps – everything needs to be numbers or converted to numbers. Many algorithms provided out of the box.

Secret Sauce:

1. Right Features (collected, extracted, engineered)
2. Right Data Preparation (scaled, normalized)
3. Right algorithm to train the model.
4. Right algorithm parameters, train/test ratios, data volume.
Secret Recipe To Devise A Good Model

1. Extract all possible features that may help to predict chargeback:
   • Static features (txn amount, email domain, address mismatch)
   • Historical, behavioral and aggregate features (avg. txn, min, max, sequences, patterns)

2. Normalize categorical or “wildly” numerical fields:
   • … | StandardScaler email_domain with_mean=false with_std=false
   • … | StandardScaler txn_value other_* with_mean=true with_std=true

3. Apply Splunk MLTK “Magic” to pick only the best features:
   • Too many features hurts model predictive ability and slows down work.
   • Too many features cause model overfitting (ability of model to make correct predictions on unseen data)
   • … | analyzefields classfield=chargeback
   • … | FieldSelector chargeback from SS_* mode=percentile param=10
Actual SPL Used To Extract Features Of Transactions

- Load data
- Set field chargeback
- Extract user email address domain
- Extract address_mismatch feature
- Extract dozen of other features
- Exclude unrelated fields
- Standardize / normalize inputs
- Extract most important features
- Fit model
index=af-cards2 sourcetype=cards2-txns

| fit StandardScaler addr_mismatch email_domain_norm with_mean=false with_std=false
| fit StandardScaler TotalTransactionValue ml_* Score with_mean=true with_std=true

| fit FieldSelector chargeback from SS_* mode=percentile param=10
| fit SVM chargeback from fs_*

- **StandardScaler** – normalize data for prediction algorithm
- **FieldSelector** – automatically select only 10% (param=10) of the most important features carrying maximum predictive qualities for the target category
- **SVM** – chosen algorithm to predict chargebacks
Secret Sauce to Predict Chargebacks

Splunk + Machine Learning Toolkit results achieved with SVM model:

Accuracy of predicting good transactions: 98.4%

Accuracy of predicting chargebacks: 90.9%
Conclusion

What helps to build successful model to predict chargebacks?

- Extracting **relevant** features for the prediction task is important. Ex: email is not important, however email domain is.

- Properly **normalizing features** (via StandardScaler and other algorithms) is important

- **Automatically selecting** only the **best features** (6-10% out of all available). Throwing away least performing features helps to minimize overfitting.

- **FieldSelector** is one of the great commands to automate field selection.

- **RiskScore** – third party input from risk calculation service did not carry any predictive value to improve chargeback detection.
Conclusion, cont.
Which features are important in predicting chargebacks?

Out of 70+ selected features – these are the ones that were automatically extracted by FieldSelector as most influential to achieve the best results in classifying transaction as chargeback:

- Address mismatch – billing and shipping addresses are different.
- Total Transaction Value.
- Email domain (Gmail, AOL, Yahoo, Hotmail, etc…)
- Number of different billing addresses used by the customer
- Number of different email addresses used by the customer
Case: Detecting Stolen Cards, Suspicious Merchants And Compromised Payment Terminals

Leveraging Splunk Enterprise and Splunk Machine Learning Toolkit to detect suspicious activity and fraud
Case study: Splunk Customer: VPNet

- Leaders in Cybersecurity for retail customers in Puerto Rico.
- Serving 65% of the credit unions in Puerto Rico.
- Leaders in Cybersecurity for the Healthcare market.
- VPNet offers innovative solutions in the telecom and IT security industry.
VPNet approached Splunk for help in detecting fraud events within debit and credit card transactions. Limited transaction logs data was provided:

- Transaction Date/Time
- Card number
- Merchant location data (State)
- Transaction type (Purchase, Cashback)
- Merchant name
- Transaction Amount
- Terminal ID

+ List of known compromised card numbers
### Payment Cards transaction log:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Transaction ID</th>
<th>Amount</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-30</td>
<td>03:35:57</td>
<td>CARD01860092</td>
<td>$41.36</td>
<td>PURCHASE, 41.36, 456560, 1441456560</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>05:29:00</td>
<td>CARD01853505</td>
<td>$81.00</td>
<td>PURCHASE, 81.00, 059820, 1664059820</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>05:34:59</td>
<td>CARD01860866</td>
<td>$169.26</td>
<td>PURCHASE, 169.26, 441223, 1266441223</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>05:40:28</td>
<td>CARD01860921</td>
<td>$65.00</td>
<td>PURCHASE, 65.00, 703340, 1832703340</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>05:45:54</td>
<td>CARD01854748</td>
<td>$5.60</td>
<td>PURCHASE, 5.60, 005557, 000005557</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>05:50:01</td>
<td>CARD01850133</td>
<td>$12.66</td>
<td>PURCHASE, 12.66, 629169, 0159629169</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>05:55:02</td>
<td>CARD01859775</td>
<td>$19.68</td>
<td>PURCHASE, 19.68, 085922, 0085922251</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>06:00:55</td>
<td>CARD01860897</td>
<td>$40.00</td>
<td>PURCHASE, 40.00, 004470, 000004470</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>06:05:45</td>
<td>CARD01860892</td>
<td>$29.52</td>
<td>PURCHASE, 29.52, 025085, 0000025085</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>06:10:45</td>
<td>CARD01854893</td>
<td>$6.98</td>
<td>PURCHASE, 6.98, 002073, 000002073, 30V8738</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>06:15:45</td>
<td>CARD01858431</td>
<td>$6.67</td>
<td>PURCHASE, 6.67, 047608, 0000047608</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>06:20:45</td>
<td>CARD01851326</td>
<td>$13.37</td>
<td>PURCHASE, 13.37, 003596, 000003596</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>06:25:45</td>
<td>CARD01855482</td>
<td>$6.38</td>
<td>PURCHASE, 6.38, 016182, 0000016182</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>06:30:45</td>
<td>CARD01854615</td>
<td>$4.25</td>
<td>PURCHASE, 4.25, 007728, 0000007728</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>06:35:45</td>
<td>CARD01860893</td>
<td>$64.04</td>
<td>PURCHASE, 64.04, 003518, 0000003518</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>06:40:45</td>
<td>CARD01860892</td>
<td>$7.61</td>
<td>PURCHASE, 7.61, 015798, 0000015798</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>06:45:45</td>
<td>CARD01860892</td>
<td>$6.70</td>
<td>PURCHASE, 6.70, 008009, 0000008009</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>06:50:45</td>
<td>CARD01860892</td>
<td>$8.56</td>
<td>PURCHASE, 8.56, 000762, 0000000762</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>06:55:45</td>
<td>CARD01860892</td>
<td>$16.21</td>
<td>PURCHASE, 16.21, 000852, 0000000852, 30V00000852</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>07:00:45</td>
<td>CARD01860892</td>
<td>$59.26</td>
<td>PURCHASE, 59.26, 009449, 00009449</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>07:05:45</td>
<td>CARD01860892</td>
<td>$44.15</td>
<td>PURCHASE, 44.15, 023491, 0000023491, 30V22933</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>07:10:45</td>
<td>CARD01860892</td>
<td>$6.50</td>
<td>PURCHASE, 6.50, 036182, 0000036182</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>07:15:45</td>
<td>CARD01860892</td>
<td>$21.66</td>
<td>PURCHASE, 21.66, 024245, 0000024245</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>07:20:45</td>
<td>CARD01860892</td>
<td>$7.40</td>
<td>PURCHASE, 7.40, 004921, 0330004921</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>07:25:45</td>
<td>CARD01860892</td>
<td>$5.24</td>
<td>PURCHASE, 5.24, 006584, 0000006584</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>07:30:45</td>
<td>CARD01860892</td>
<td>$18.37</td>
<td>PURCHASE, 18.37, 012170, 0000012170</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>07:35:45</td>
<td>CARD01860892</td>
<td>$15.00</td>
<td>PURCHASE, 15.00, 264381, 00000264381</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>07:40:45</td>
<td>CARD01860892</td>
<td>$7.63</td>
<td>PURCHASE, 7.63, 028541, 00000028541</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>07:45:45</td>
<td>CARD01860892</td>
<td>$28.67</td>
<td>PURCHASE, 28.67, 005932, 0330005932</td>
</tr>
</tbody>
</table>
1: Detailed Transactions Dashboard

Dashboard allows to do necessary filtering and searching for transactions data.
**1: Detailed Transactions Dashboard**

Dashboard allows to do necessary filtering and searching for transactions data.

### Payment Cards: Detailed Transactions

<table>
<thead>
<tr>
<th>Time</th>
<th>Card number</th>
<th>Card risk score</th>
<th>Compromised payment card</th>
<th>Invert risk</th>
<th>Invert risk message</th>
<th>Risk</th>
<th>Merchant</th>
<th>Merchant change</th>
<th>Merchant name</th>
<th>Terminal ID</th>
<th>Terminal dem.</th>
<th>Amount</th>
<th>Terminal ID</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/08/2017 11:44:27</td>
<td>CARD01001</td>
<td>0.00</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>1</td>
<td>5963</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/08/2017 11:44:27</td>
<td>CARD01002</td>
<td>0.00</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>1</td>
<td>5896</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/08/2017 11:44:27</td>
<td>CARD01003</td>
<td>0.00</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>1</td>
<td>3963</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/08/2017 11:44:27</td>
<td>CARD01004</td>
<td>0.00</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>1</td>
<td>5963</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01/08/2017 11:44:27</td>
<td>CARD01005</td>
<td>0.00</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>1</td>
<td>5963</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Detailed filtering and searching**

**Suspicious transactions marked in red**
Detecting Suspicious Transactions With Splunk

How we can detect suspicious transactions?

1. We know approximate location of each transaction. In this case: State
2. If time between 2 adjacent transactions is too small considering their physical location – Alert!

<table>
<thead>
<tr>
<th>Time delta between transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merchant</td>
</tr>
<tr>
<td>Txn State</td>
</tr>
<tr>
<td>Txn type</td>
</tr>
</tbody>
</table>

Splunk detected suspicious transaction passed at a physical location within impossibly short time from transaction done in another state

<table>
<thead>
<tr>
<th>Order of Txns: Newest on top</th>
</tr>
</thead>
</table>
How To Detect Suspicious Transactions With SPL

| sort 0 card_id, _time
| streamstats window=2 current=1
  dc(txn_region) as region_change,
  dc(merchant_name) as merchant_change,
  range(_time) as time_delta
by card_id

| eval region_change=region_change-1, merchant_change=merchant_change-1

| eval risk_1_triggered=if(region_change>0 AND time_delta<7200, 1, 0)
| eval risk_2_triggered=if(merchant_change>0 AND time_delta<60, 1, 0)
2: Cards Risk Summary Dashboard

Allows executive to see current overall exposure to risk based on activity patterns.

Dashboard offers single view of all risky and compromised cards sorted by risk score. Activity summary is shown for each card.
3: Merchants and Payment Terminals Analysis

Detect anomalies of card usage at specific merchants and payment terminals

Risk scoring of merchants and payment terminals that process excessive amounts of compromised and risky behaving payment cards.
3: Merchants and Payment Terminals Analysis, cont.

Detect anomalies of card usage at specific merchants and payment terminals

Analyzing suspicious payment terminals that process anomalous number of compromised cards vs. other cards
4. Detecting Anomalous Behaviors

Applying unsupervised learning techniques to detect anomalous behavior and new, previously unknown fraud patterns

We want to be able to aggregate multidimensional behavior of all payment cards together to discover unusual, potentially risky or fraudulent behavior.

We need to simultaneously analyze multiple characteristics of all cards and all transactions and all behaviors to detect outliers and prevent potential losses.

Applying unsupervised learning techniques to detect anomalous behavior and new, unknown fraud patterns.

“Normal” or typical behaviors are grouped together.

Anomalous behaviors stand out from the majority of the crowd.
Detecting Anomalies Via Clustering
Applying Machine Learning Toolkit clustering to filter our anomalies

```
index=vpnet2 sourcetype=cards_txn2
| where len(txn_region)>0 | dedup _raw | sort 0 card_id, _time
| streamstats
  window=2 current=1 dc(txn_region) as region_change,
  dc(merchant_name) as merchant_change, range(_time) as time_delta by card_id
| eval region_change=region_change-1, merchant_change=merchant_change-1
| where time_delta>0 | eval x="Throw away oldest event for each card"
| stats c as num_txns
  max(txn_amount) as F_txn_amt_max, avg(txn_amount) as F_txn_amt_avg, stdev(txn_amount) as N_txn_amt_std
  median(txn_amount) as F_txn_amt_median, avg(time_delta) as N_td_avg, stdev(time_delta) as N_td_std
  c(eval(merchant_change>0)) as merchant_changes_num c(eval(region_change>0)) as region_changes_num
  by card_id
| where num_txns>=5
| eval F_merchant_changes_num_norm = merchant_changes_num / num_txns
| eval F_region_changes_num_norm = region_changes_num / num_txns
| eval F_txn_amt_std_norm = N_txn_amt_std / F_txn_amt_avg
| eval F_time_diff_std_norm = N_td_std / N_td_avg
```

Get data!
Create SPL search
Extract needed features
Detecting Anomalies Via Clustering, Cont.

Applying Machine Learning Toolkit clustering to filter our anomalies

1. Apply preprocessing steps to normalize features
2. Define clustering algorithm

- fit StandardScaler F_*
- fit PCA SS_* k=3
- fit KMeans PC_1, PC_2, PC_3 k=18
Detecting Anomalies Via Clustering, Cont.

Applying Machine Learning Toolkit clustering to filter our anomalies

Get generated SPL code
Detecting Anomalies Via Clustering, Cont.

- Splunk Machine Learning Toolkit assigns data to **different clusters**.
- One way to find the most anomalous data elements is find the smallest, most isolated clusters of data.
- Smallest and most isolated (anomalous) clusters of data often contain patterns of attacks, suspicious and fraudulent activity.
Detecting Anomalies Via Clustering, Cont.

- Smallest clusters in this data representing real world dataset of credit card transactions containing patterns of suspicious activity.

- Anomalous clusters immediately shows
  - Cards with unusually high transactions values
  - Cards containing “fast region shift” fraud pattern.
  - Cards with unusual geo travel patterns

- No pre-programmed rules being used.
Detecting Anomalies Via Clustering, Cont.

- Splunk can detect anomalies in payment card transactions in close to real time.

- Most essential anomalies can be “bubbled up” for analysis and review.

- Automated alerts about detected anomalies can be sent:
  - to multiple fraud analyst teams via email alerts.
  - to Splunk Enterprise Security via “notable events”
  - to another system via script / API calls.
Summary Notes And Conclusions

Above fully custom fraud detection app:
- Built with Splunk Enterprise
- No coding, only Simple XML was used
- No coding, everything was done via Web interface
- Was built by 1 person
- Was built in 7 days time

Splunk Machine Learning Toolkit allows to apply both supervised and unsupervised learning techniques on top of any data.

Payment cards fraud and any kind of suspicious activity can be predicted

Known and Unknown Fraud = always anomaly. The secret of detecting known and unknown fraudulent patterns is to:
- Have access to as much data as possible
- Extract relevant features of behavior
- Apply and combine anomaly detection techniques available on top of data

Splunk Machine Learning allows to learn from data and generalize from complex data examples to predict outcomes (such as fraud, chargebacks, etc…)

Splunk Enterprise allows building of advanced, fully customized security and anti-fraud solutions in a short period of time.
Detecting Credit Card Fraud on Credit Unions

Preventing fraud by analyzing data on Splunk with Indicators of compromise

Felipe J. Hernandez, CEO, VPNet Inc
VPNet offers innovative solutions in the telecom and IT security industry.

Serving customers across all the industries from Retail to banking.

- Leaders in Cybersecurity for retail customers
- Serving 65% of the credit unions in Puerto Rico
- Leaders in Cybersecurity for the Healthcare market

Our success and having contracts with reputable companies in Puerto Rico, it is directly related to our commitment with the quality and excellent customer service.
Debit Card Fraud in Credit Unions
The Problem: MasterCard Brand debit cards suffering from massive fraud issues

Impact:
- Debit card losses not protected by MC Credit insurance
- Losses not covered by local clearing house
- Credit union covering 100% of the losses
- Big impact on CU image plus inconveniences for customers
- High cost of replacement of compromised cards, average of $35 per replacement
Only Limited Tools Available To Protect Credit Unions

Technical tools:
- Using technical tools to stop transaction based on human suspicion:
  - Falcon
  - TEXT message
  - MC interface to block countries and vendors
  - Limited spending control

Business intelligence tools:
- Transactional Data history N/A
  - No average transaction amount, 20pt
  - No demographic info
  - NO spending patterns
  - NO risk assessment of customers
How We Could Help Credit Unions?

Creating a tool that would help them minimize their risk that would:

- Provide historical Data on users
- Spending patterns
- Other IOC’s that could create a riskier profile
- Using Machine learning creating a self adjusting credit risk based on behavior
- Locate which stolen cards have not been identified yet as compromised!!!
How We Could Help Credit Unions, Cont.

We need to consider:

- New compromised cards would pop up every day.
- The exposure was totaling near $300k.
- Still no clear idea on how the breach happened.
- Since all cards couldn't be voided simultaneously a maximum expending allowance was needed for users that were not classified as compromised yet, but where in risk. This allotment was going to be based on their risk score.
Getting The Data

- Live data wasn't useful without a historical perspective
- All historical data was provided in archived and proprietary form, so significant reformatting had to be done.
- We needed Gleb urgently!!
- Once historical data was inserted into Splunk, we started seeing patterns that were very insightful
- From now on Splunk stream will provide access to live data.

Crunch time!!!
What The Numbers Told Us?

- Many cards that were not reported as compromised by users
- Patterns used by fraudsters to test the cards and not alert the owner
- Merchants that were being used for the transactions
- POS used for the purpose
- POS where cleared out as the source of compromise.
- At that point data was either extracted from the institution or leaked at the clearing house level.
- Later after receiving data from other institutions that had some fraud as well, the same POS’s were also used with cards of other institutions, proving that the problem wasn’t one of breaching at the CU.
- Many cards that were not reported as compromised by users
Patterns Of Fraudsters

- Tested the cards 90 days before the massive charges.
- Tested with small Amounts, 2-5 Dollars in average.
- Tested on common merchants like Walgreens, Costco and Target
- They used the same POS’s (possibility of complicit behavior with cashiers).
- Use the cards to purchase Gift Cards and other debit cards to sanitize the money.
- As soon as they noticed that some cards quit working they stopped transacting and waited a few days before continuing their use.
- Typically the transaction average was $500 but the amount would vary dependent on their sense of being traced.
Splunk Benefits For VPNet

▶ One platform for all of our security elements
▶ Single point to manage all of our data intake
▶ One platform to manage and measure all data, from security events to interactions on our Social-Wifi Network.
▶ Opportunity to monetize our Data.
▶ Create Business intelligence solutions for customers
▶ Move all critical elements of our operations into Splunk
What’s Next?

► Integrate Splunk STREAM as the basis of data collection for all customers
► Move the monitoring to our SOC
► Use machine learning for risk scoring to achieve automatic transaction blocking or establish funds limits.
► Create a full suite of business intelligence products.
► Integrating Splunk on Credit Unions for all their statistical analysis including marketing and members behavior.
► Expand services to all Caribbean countries
Happy Splunking!
Thank You

Don't forget to rate this session in the .conf2017 mobile app