Monitoring consumer credit card transactions

Banks want real-time details regarding their credit cards to optimize operations. As a retail bank analyst, you need insight into attempts that are authorized, cancelled, or denied, mapped to customer experience with regards to response time. Knowing in near real-time the status of credit card usage is an important banking function.

Data required

Business service data for credit card transactions

Procedures

• Splunk recommends that customers look into using data models, report acceleration, or summary indexing when searching across hundreds of GBs of events in a single search. The searches provided here are a good starting point, but depending on your data, search time range, and other factors, more can be done to ensure that they scale appropriately.

• Your typical banking transactions may include more than four steps, and some commands, parameters, and field names in the searches below may need to be adjusted to match your environment. In addition, to optimize the searches shown below, you should specify an index and a time range when appropriate.

► Credit card authorization issues

A customer or entity may cancel a credit card authorization attempt and some customers may receive errors. Some may initiate the authorization again. Each of these KPIs needs to be noted to see how many times they occur in a given time period.

Customers with cancellations or errors

```
|sourcetype=<credit card transaction data source>
| eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
| sort _time
|where action="cancelled"
|table _time, customer, action, amount, subcontractor
|eval amount=tostring(round(amount, 2),"commas")
```

You can change the action in the where command to "error" or any other status you are interested in.

Customer with cancellations followed by an authorization

```
|sourcetype=<credit card transaction data source>
| eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
| sort _time
|stats values(amount) AS amount first(action) AS first_action last(action) AS last_action by customer,
```

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
subcontractor, sessionID  
|where first_action="cancelled" AND last_action="authorized"  
|eval amount=tostring(round(amount, 2),"commas")

► Credit card authorizations today versus yesterday

Banks want to know the average response time day over day for credit card authorization attempts. This search provides a report that compares one day to the day before. If the chart changes dramatically and nothing else has changed, investigate why.

|sourcetype=<credit card transaction data source>  
|eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")  
|sort - _time  
|timechart span=15m fixedrange=F avg(ResponseTime) AS ResponseTime  
|timewrap series=exact time_format="Hours of %m/%d" 4h

► Credit card usage counts by authorization status

Credit card authorization attempts can lead to authorized, denied, cancelled, or error response actions. Each subcontractor (partner) who licenses the credit card provides a status. These statuses can be summed up by subcontractor and shown. This search is very useful to monitor the business. If a particular subcontractor has too many credit card issues, they will show up on this report, indicating proactive action should be taken.

|sourcetype=<credit card transaction data source>  
|eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")  
|sort - _time  
|chart count OVER subcontractor BY action

► Credit card usage highest response times

This example shows a report of customers who have the highest response times for credit card authorization attempts in a given time compared to the rest of the customers. By finding response times greater than the average of all response times plus N*standard deviation, no hard-coded threshold is needed. The business should be aware of these outliers. Knowing which customers are suffering the worst customer experience may be the first step to improving it.

|sourcetype=<credit card transaction data source>  
|eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")  
|sort - _time  
|stats avg(ResponseTime) AS averageResp BY customer, subcontractor  
|eventstats avg(averageResp) AS avg stdev(averageResp) AS stdev  
|where averageResp>(avg+4*stdev)

► Credit card usage top customers’ authorization counts

This search shows a report of customers who have the highest amount of successful credit card authorizations in a given time compared to the rest of the customers. By finding counts greater than the average of all attempts plus...
N*standard deviation, no hard-coded threshold is needed. Your business should be aware of its highest usage customers.

\[
\text{sourcetype=<credit card transaction data source>}
\text{where action="authorized"} \text{eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")}
\text{eval amount=tostring(round(amount, 2),"commas")}
\text{stats count values(amount) AS amounts values(subcontractor) AS subcontractors BY customer}
\text{eventstats avg(count) AS avg stdev(count) AS stdev}
\text{where count>(avg+2*stdev)}
\text{| sort - count}
\]

Credit card authorization response times by subcontractor

Comparing the average response time for credit card authorization attempts over time split by subcontractor can be used to understand the customer experience with subcontractors. If any of the subcontractors have response times much worse than the others, you should follow up.

\[
\text{sourcetype=<credit card transaction data source>}
\text{eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")}
\text{sort _time}
\text{|timechart span=10m fixedrange=F avg(ResponseTime) AS averageResponseTime BY subcontractor}
\]

Credit card authorizations and denials by subcontractor

Subcontractors for credit card authorization provide response action statuses (such as authorized versus denied) over time. By providing a report on actions over time, your bank can gauge the performance of their underwritten cards issued to their partners. Too many denials or not enough authorizations should lead to an investigation.

\[
\text{sourcetype=<credit card transaction data source>}
\text{eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")}
\text{sort _time}
\text{|timechart span=10m fixedrange=F count(eval(action="authorized")) AS authorized}
\text{count(eval(action="denied")) AS denied BY subcontractor}
\]

Credit card authorization counts by subcontractor

These searches show reports for actions (authorization, cancellations, etc.) by subcontractors with absolute counts, counts over time, and counts split by action. The reports can be given to executives to gauge business performance.

Count by authorizations over time

\[
\text{sourcetype=<credit card transaction data source>}
\text{eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")}
\text{sort _time}
\text{|timechart span=10m fixedrange=F count(action) AS action BY subcontractor}
\]

Count by possible actions

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Next steps

Use the results of these searches to evaluate service and capacity and make business recommendations. You should put these results on a dashboard that is available to executives so the business can make decisions in real-time to react to unusual conditions. Proactively monitoring authorization issues may help improve the application and business process. When taking action on these results, be sure to follow any industry policies and regulations that are required for compliance.

The Splunk Essentials for the Financial Services Industry app helps you automate the searches provided in this article. The app also provides more insight on how they can be applied in your environment, how they work, the difficulty level, and what data can be valuable to run them successfully. In addition, the Splunk Essentials for the Financial Services Industry app provides a number of other monitoring and reporting solutions for financial services:

- ATM usage statistics
- Wire transfer statistics
- Retail banking transactions

You might also be interested in monitoring credit card transactions for potentially fraudulent activity.

If you have ITSI, a Glass Table showing at a glance credit card authorization and other KPIs can provide instant feedback on the health of your authorization application. Create an App Server Service that has requests for credit card authorizations as a KPI in ITSI. Create another service that fulfills the authorization requests. The App Server Service Health depends on the KPI that fulfills the authorization service. Create thresholds for critical, high, medium, and normal for each KPI. Create a Glass Table that shows the App Server and Authorization Service with a minimum of the 2 KPIs and enhance it to use Adaptive Thresholds and also have dependent services in the Glass Table.

Finally, these additional Splunk resources might help you understand and implement this use case:

- .Conf Talk: 40 ways to use Splunk in financial services