FIRST PERFORMANCE
GLOBAL

SUCCESS STORY
Regional Processor

MINIMIZE FRAUD EXPOSURE

> *The First Performance solution enables us to offer features and functionality that minimizes fraud exposure and adds an extra layer of security for cardholders.*
>
> *~ Processor Executive*

BACKGROUND

Our customer, a regional payment processor, deployed the First Performance solution at six local banks. The features, which are accessible from the bank's mobile app, provide financial institutions and their customers with self-service capabilities to increase digital engagement and satisfaction.

CHALLENGE

With global card fraud on the rise and forecasted to reach $38 billion by 2024, our customer wanted a solution that offered protection for financial institutions and their customers. Finding a solution that delivered self-service controls, alerts, and added security was paramount

Experiencing a fraud event without protection, could compromise the trust and loyalty of cardholders, exponentially increase call center volume, and incur significantly higher fraud exposure and cost.

SOLUTION

- **Deployment Type**: API Deployment
- **Deployment Model**: Hybrid (Combination of On-Premise and Cloud)
- **Key Features**: Real-time Card & Channel Controls, Transaction-Based Alerts, Admin Portal and Call Center Management Portal
- **Portfolio Type:** Consumer Credit
- **Enrolled Cards**: 79% of the Total Credit Card Portfolio

FRAUD INCIDENT

In July 2018, there was a data breach where hackers gained access to 14,000 credit card numbers and published the card numbers, expiration dates, and security codes on the dark web.

RESULTS

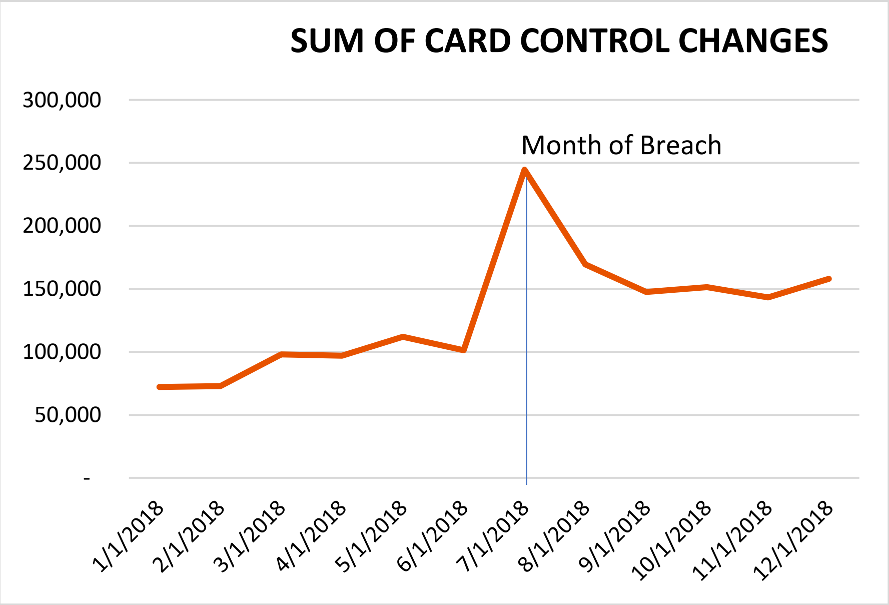
The fraud incident demonstrated that the platform helped to minimize fraud exposure, avoid high levels of call volume into the bank's customer service center, and provided cardholders with self-service controls that allowed them to take immediate action to turn their credit cards off via their bank's mobile app.

Incident went Public July 25, 2018

6 Banks Live on FP Platform

14,000 Cards Compromised

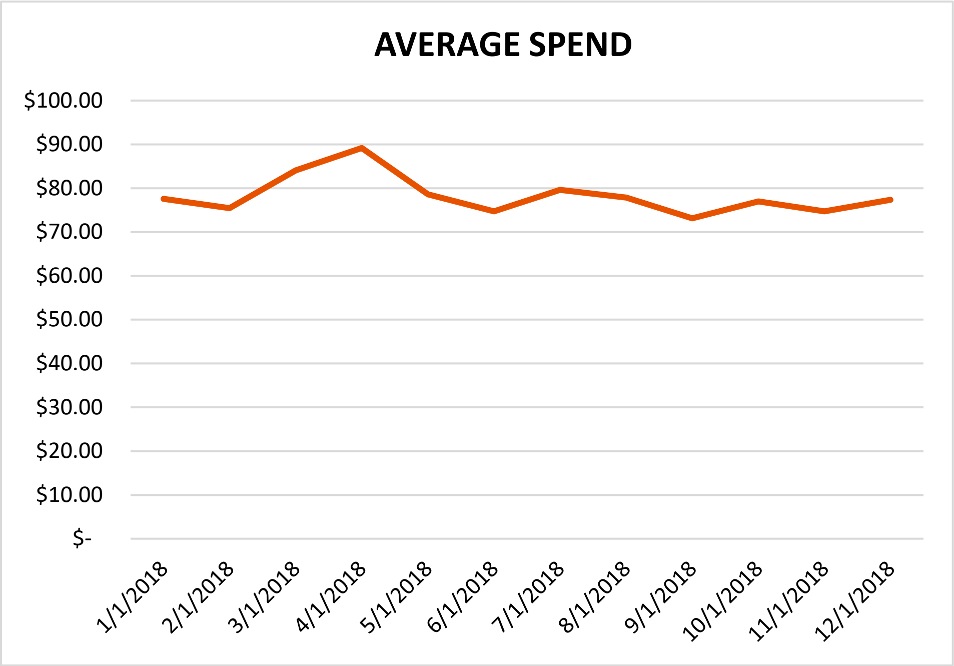
SELF-SERVICE CARD SETTING CHANGES



241% Spike in Usage

67% Post Event Usage

NO IMPACT ON SPENDING



Cardholders took action before banks

99.5% of setting changes from self-service

No noticeable impact on spending after the incident

No impact on card usage, spend, and associated bank interchange revenue, due to cardholder's self-service management to continue to be able to safely transact with their card.

CONCLUSION

Taking a proactive approach and implementing advanced technology has proven to address and minimize the cost and cardholder impact of fraud.

Financial Institutions:

- Minimized fraud exposure and costs
- Reduced attrition and improved the user experience
- Minimized the impact on the call center and associated expenses

Cardholders:

- Use real-time controls to protect themselves against fraud
- Continued use of their card to make important purchases
- Felt more secure and satisfied with their bank

ADDED PROTECTION – *MINIMAL EXPOSURE* – *SATISFIED CUSTOMERS*