US based community bank with 15,000 retail banking users and 400 business banking customers.

Challenges

This bank offers a full spectrum of banking services and wants to expand online and mobile banking capabilities without exposing themselves or their customers to accompanying online fraud risk.

Fraud Risk

The bank wanted to take a proactive approach to securing their online and mobile channels. It started with the fundamental premise that all end points are compromised and just having security education for account holders would not be an effective risk mitigation strategy.

Business Case

It was obvious that even a single fraud event can cause ripple effect across their internal operations, their bottom line and their position in the market. By investing in a fraud prevention solution, the bank would be able to:

- Enhance existing customer relationships and build trust as both can crumble in an instant as a result of a fraud attack
- Maintain their hard--earned reputation, the heart and soul of any community bank.
- Optimize limited staff resources by avoiding the manic scramble that inevitably accompanies any fraudulent transfer.

Solution

Following are the key points for the bank to accept a solution:

- Defend against the growing variety and sophistication of fraud threats across multiple end points.
- Transparently protect all account holders.
- Proactively identify suspicious activity instead of waiting for a fraudulent transfer to happen.
- Low operational impact.

Based on these criteria, Dynapt provided behavioral analytics solution that met all of the criteria they established and utilized the key strategic advantage the bank has over the fraudsters i.e. knowledge of their customer's behavior. With the solution Dynapt provided, the bank could use rich histories of online behavior to detect anomalous activities and unusual transactions at the individual account holder level. For example, a multiple times login attempt and then transaction

of 9x amount where x is the average transaction amount could be a potential fraud, so the bank would send an OTP to the user for anymore transaction.

Results

The bank has shifted from reactive to proactive mode, identifying suspicious activity before the money is transferred or enabling proper re-authentication in similar cases. The bank has improved fraud prevention capabilities alongside expanding online and mobile banking services. It has strengthened customer relationships while improving their value proposition for new customers.

Proactively prevent fraud:

- 15,000 consumer banking users and 400 business banking customers are now receiving improved protection and service, without any inconvenience or added burden.
- Uses behavioral analytics to establish unique “impressions” of each user, monitor all online sessions to spot anomalous activity, report the highest risk accounts for any fraud events.