The Fraud Management Hub: No Such Thing As Too Many Tools
# TABLE OF CONTENTS

Overview .................................................................................................................. 3

Fraud Solution Overload ......................................................................................... 3

The Cyber-Fraud Challenge ...................................................................................... 3

How Fraud Management Hubs Tackle the “Too-Much-Information” Challenge .................................................................................................................. 4

Extending the Existing Investment; Preparing for Growth ........................................ 5

Starting Small with Mini-Hubs .................................................................................. 5

Example Use Cases for Mini-Hubs ........................................................................... 5

What is the Best Fraud Management Hub for Me? .................................................. 6

ABOUT NICE ACTIMIZE ......................................................................................... 6
Overview

It seems impossible to apply the phrase “too much information” to fraud detection. After all, the more information we have on customers, transactions, banking histories, and devices, the easier it should be for financial institutions (FIs) to detect fraud. The problem is that FIs use dozens of disparate point products and solutions that produce separate outputs and alerts. For most FIs, this uncorrelated data is not quite as effective as it would be if it were viewed within one context and used together to understand risk, streamline investigations and operations. Eliminating best-of-breed point products is not the answer. Instead, FIs can make these products work better together using an integrated platform – or fraud management hub – that can ingest all of the outputs and incorporate it into a unified detection and investigation strategy.

Fraud Solution Overload

The past five years have been marked by FI innovation. Institutions have taken radical steps to improve customer experience by opening up self-service touch-points through online and mobile banking channels. Banks have also enabled speedier settlements in deposit, payment, and money transfers; all the while aiming to eliminate customer friction -- fewer calls to the customer, fewer hard limits on account access.

As these new channels develop, banks also risk opening new opportunities for fraudsters to exploit. Individual, point-product fraud solutions that can protect specific channels, transaction types or use cases have piled up as a result. Today, a very large bank commonly has upward of a dozen fraud and cyber detection tools in a single banking channel.

The resulting abundance of tools can lead to a host of operational inefficiencies. Employees spend more time managing many separate systems, and this maze of sometimes overlapping alerts and data leads to complicated or even unnecessary investigations. Even more concerning, overlapping investigations can lead to poor customer service -- unnecessarily shutting off access to accounts or placing multiple calls to users for the same event.

The Cyber-Fraud Challenge

Every data point is a clue in preventing and solving the fraud problem. Beyond navigating between multiple financial crime solutions, banks are also implementing tools to handle the effects of cyberattacks across their relevant banking channels. FIs can now consider a host of information about their customers ranging from device ID and network connection to geolocation and navigation history. These cyber and financial crime tools create a host of separate clues, however, when this information is correlated, institutions are able to identify a holistic cyber-fraud picture with a clearer and more effective view of the fraud detection and prevention process.
How Fraud Management Hubs Tackle the “Too-Much-Information” Challenge

A fraud management hub strategy allows banks to ingest data from multiple fraud and cyber tools to create richer analytics profiles, risk models, scores and, alerts. Ultimately, banks gain a holistic picture of the customer and an improved ability to spot behavior anomalies.

The cornerstone of an effective fraud hub is data – or specifically the ability to ingest large sets of information from disparate fraud and cyber tools and map it into existing or customized fraud risk models. FIs gain a cross-vendor, real-time data management system and a unified strategy that changes the way they handle analytics, operations, and decisions.

The hub’s analytics engine integrates scores from all of the disparate tools into existing fraud models to create a “score of scores” scenario. The combined data is used to dynamically create customized profiles and predictive models. FIs can immediately and automatically process the vast majority of good customers and transactions, and focus their risk models on the much smaller percentage of risky cases.

The fraud management hub strategy can be extended to apply centralized policy and control to make effective decisions using combined cyber and fraud information. Without overlapping alerts and disparate investigations, fewer false positives, second-calls to customers and unnecessary hard limits, centralized decision-making improves the customer experience.

The fraud hub optimizes the way FIs manage investigations and cases by supporting consolidated investigation and case management. With a centralized view of investigations and workflows, the system manages the process from the initial alert through to case resolution.
Extending the Existing Investment; Preparing for Growth

Using a fraud management hub, for holistic models, scores and alerts, can extend the value of existing investments in best-of-breed point products. These individual fraud and cyber tools are great at monitoring and collecting data to detect problems in very specific channels or scenarios, but do not bring with them broad analytics models or workflow and case management. By integrating data from these tools into risk models, a fraud management hub makes these tools part of a broader analytics strategy. The hub streamlines management and investigations to otherwise simple tools - suddenly a small solution has a whole lot more might. Considering that most banks will only continue adding point products as they increase innovation and diversify their services, the hub helps to ensure scalability in the future.

Starting Small with Mini-Hubs

Moving into a fraud management hub strategy does not have to be an enterprise-wide undertaking. The implementation of mini-hubs that more narrowly focus on specific channels or functions allows an FI to start small. For example a mini-hub could be used solely for data or alert management by ingesting alerts from many tools across channels to avoid overlap. Other example might focus a hub on a single channel and use case, such as mobile log-ins and authentication. These mini-hubs can eventually connect into a larger, interconnected platform if required, but they are useful and effective as standalone options.

Example Use Cases for Mini-Hubs

<table>
<thead>
<tr>
<th>Example Use Cases for Mini-Hubs</th>
<th>How It Works</th>
<th>The End Result</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log-On and Authentication</strong></td>
<td>Ingests cyber tools data, such as malware history and device ID, and integrates this with banking information from fraud detection tools, such as payment amount, customer transaction history, and payee identification.</td>
<td>Limit unnecessary multi-factor authentication by applying fraud analytics to the much smaller incidence of risky behavior.</td>
</tr>
<tr>
<td><strong>Call Center Fraud Management</strong></td>
<td>Suspicious activity detection tools consider everything from device ID to call session analysis and voice biometrics.</td>
<td>Authenticate monetary or service change events in real-time, ensuring that fraudulent attempts are stopped on contact.</td>
</tr>
<tr>
<td><strong>Holistic Digital Banking</strong></td>
<td>Ingest data from cyber and fraud tools. Apply combined data to risk models and decisions specifically relating to digital transactions – P2P, bill pay or money transfer.</td>
<td>Gain a holistic, cross-channel view to make better, more efficient decisions without sacrificing customer experience.</td>
</tr>
</tbody>
</table>
What is the Best Fraud Management Hub for Me?

The short answer is that there is no universally perfect fraud management hub. Each hub unifies a different set of existing tools and applies risk models accordingly. Every institution will have a different set of needs and requirements that determine the best hub strategy for them, one that integrates their point-product specific data into a holistic cyber-fraud strategy, streamlines management and operations, and improves customer experience.

The sky is the limit as FIs begin to experiment with cyber-fraud hub use cases. Whether an FI starts by tackling extremely specific challenges or begins with an enterprise-wide, integrated data and management hub, this is an exciting time for fraud prevention professionals looking to maximize their investments and their effectiveness.