customer care solutions
from Nuance

NUANCE

case study ::

International Retail Bank Reduces Fraud with Proactive Notifications from Nuance Notification Hub

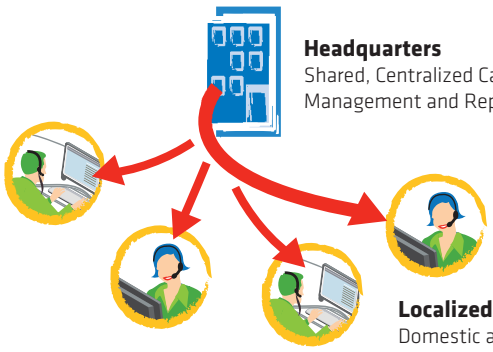
the company

An international retail bank has thousands of offices worldwide and over a dozen contact centers serving their customers. Their commitment to excellence in customer care has earned their contact centers numerous awards.

the challenge

The response to possible bank card fraud is one of the most important factors affecting the relationship that customers have with their bank. For customer-centric financial institutions who issue millions of bank cards, any instance of possible fraud is both a business risk to be managed and an opportunity to strengthen customer relationships. To help identify these financial risks the bank uses a third party fraud detection system that issues real-time alerts on unusual card activity. In the past, these alerts were sent directly to the bank's highly trained Bank Card Security specialists who would manually call customers and work with them to verify and resolve the suspicious card activity. They would then update the CRM system so the interaction was included in the customer record. Although customers appreciated the proactive approach and the bank reduced losses due to fraud, the specialists were spending unnecessary time dialing and trying to reach customers rather than working to reduce fraud.

Bank Headquarters and Localized Contact Centers



Headquarters
Shared, Centralized Campaign Management and Reporting

Localized Agent Pool
Domestic and International

Distributed Architecture
- Meet the Needs for Domestic and International Customers
- Localized Efficiencies and Staffing
- Centralized Management
- Economies of Scale

The daily volume of alerts on compromised cards fluctuates. In order to handle spikes in volume beyond the capacity of the Bank Card Security specialists, the bank would send the overflow to local contact center agents to make the outbound calls and work with the customer. The contact center managers, however, found it difficult to optimize their operations with this unpredictable demand on their staff.

For the occasional times when there were a huge number of alerts, such as a security breach of a major retail merchant, the overflow would also be sent to the local branch offices to follow up with the customer. The local offices often could not react immediately and make these outbound calls as they were already servicing customers directly.

The bank realized that capacity concerns and inefficiencies in their alert notification process were limiting their ability to reduce fraud. To address these operational challenges, they needed a comprehensive solution where:

- Security specialists spend their time on fraud reducing activities rather than dialing customers and leaving messages
- Proactive notifications can always be sent to customers even when there are large spikes in activity
- Contacting customers for security purposes is a global responsibility shared across all contact centers
- Customer relationship management (CRM) and management reporting systems always track the most current customer interactions

To solve these challenges with a global focus, the bank required an automated proactive notification solution that offered the efficiencies of centralized control and yet had the flexibility for local contact centers to deliver a personalized customer experience. Also crucial to success, the solution needed to leverage existing telephony investments and to seamlessly integrate into the bank's existing real-time business processes.

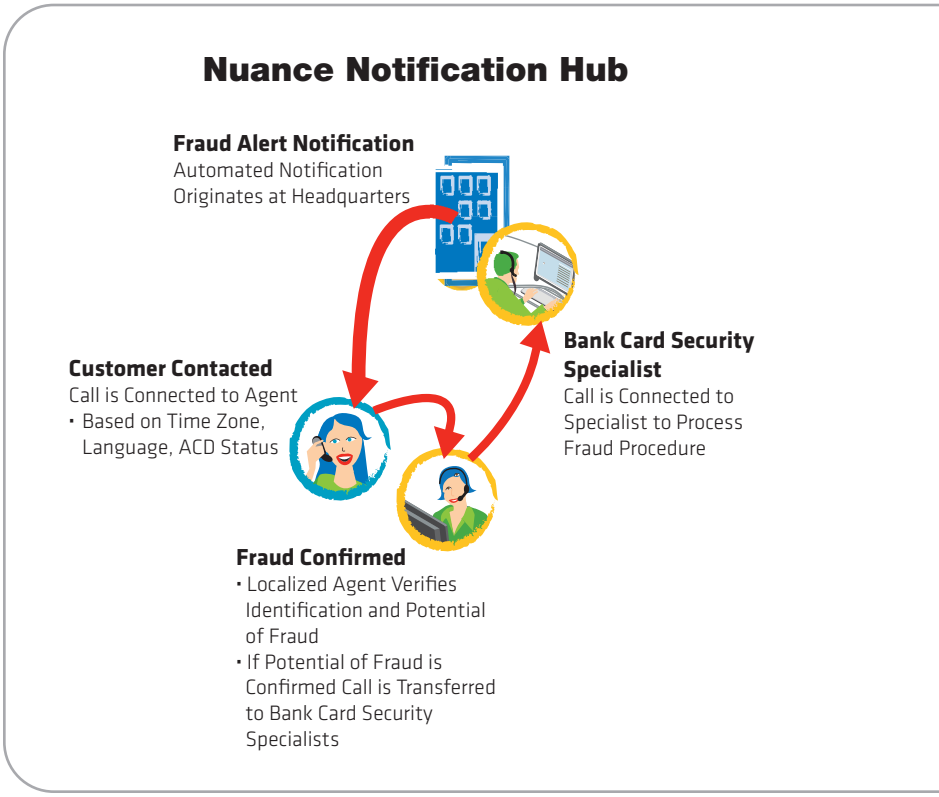
the options

To find a solution, the bank first considered the automated outbound calling technologies that were available in other areas of the company. These were conventional predictive dialers designed to support collections and telemarketing campaigns. Although the predictive dialers were capable of placing high volumes of calls, they relied on batch-oriented processes for caller information making them not well suited for the real-time needs of the fraud alerts process. Similarly, the predictive dialers were incapable of generating real-time updates into the CRM system used in all contact centers and offices, severely limiting the CRM's effectiveness in supporting a dialogue with the customer at a very sensitive time in the relationship.

Having ruled out the existing technologies, the bank decided a new *universal notification platform* would be needed that all business units could use. This scalable platform would integrate their unique business rules and applications to send multi-channel proactive messages tailored to their business and customer needs.

the solution

The bank selected the Nuance Notification Hub to be the cornerstone of their universal notification platform. Having worked successfully with Nuance on previous self-service and CTI projects, the bank knew Nuance would be willing to partner closely with them and take the time to understand their needs on this important fraud reducing effort.



The bank has deployed the Nuance Notification Hub (NNH) as a complete proactive fraud management solution, known internally as the *Alerted and Compromised Card Notification* initiative. All aspects of the fraud notification process are designed, managed, and analyzed using NNH. Taking advantage of economies of scale, the system is operated from the main data center and runs campaigns throughout their global operations. The openness of the system allows it also to be tightly integrated with the bank's core applications and to drive local business rules for these applications.

The alert and notification process begins with the third-party fraud detection system sending an alert directly to NNH to look-up how each customer prefers to be notified about this alert, taking into account language and time of day. For customers opting for email or SMS, a personalized message is immediately sent and the customer's CRM record updated, including if the message bounced or could not be delivered. Much more common though is for NNH to place a call directly to the customer. If an answering machine picks up, the bank has business rules defined to only leave a message after the third attempt, but noting each attempt in the CRM record. Each voicemail message includes a personalized greeting and customer specific information. Commenting on the scalability of the system, the bank's VP of Banking Solutions said ***"without this technology, we'd still be calling a lot of customers"*** affected by the theft from a large merchant of information on millions of their bank card customers.

When customers do answer the call, they are verified and presented with a personalized dialog informing them of the possible fraud incident and offering to connect them with an agent to resolve it. Taking advantage of sophisticated scheduling and CTI, NNH then identifies the appropriate local contact center and the most suited agent in that center. The bank has also been able to increase the utilization of their contact centers by defining unique business rules in NNH. They throttle the volume of outbound messages sent depending on the available capacity of contact centers to handle the expected inbound call volume generated when customers receive alerts. The volume of outbound calls is reduced during peak inbound call times and increased during non-peak times to make better use of their existing resources and investments.

NNH then connects the customer with the agent, along with passing the alert information. The agent quickly determines if the fraud alert is valid. For example, an alert may be

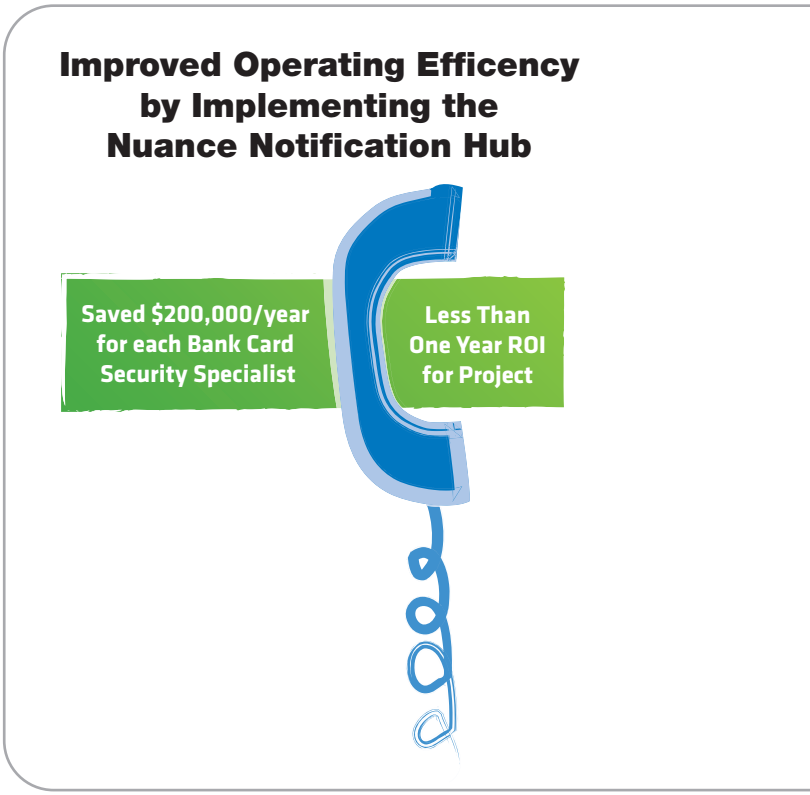
The Alerted and Compromised Card Notification System

Alerts Sent to Customer-selected Method of Communication

triggered if the same bank card was charged a large amount twice within an hour for gasoline at different locations. The agent would simply ask if the customer made these charges. If fraud is suspected, the customer and alert information are directly transferred to an appropriate Bank Card Security specialist to resolve the incident and complete the process.

the results

Implementation of an automated proactive notification process using Nuance Notification Hub has enabled the bank to reduce risks from fraud by enabling fraud specialists to be focused on resolving fraud rather than initial customer contact activities. The bank estimates the direct impact for this improved efficiency to be more than $200,000/year for each of their Bank Card Security specialists. The return on investment for the project was less than one year, leading to positive internal recognition for the project team.



In addition to the direct financial impact from the fraud specialists, the managers of the local contact centers have enjoyed other tangible results. By associating the timing of outbound notifications to take advantage of unused capacity, the contact center manager's own performance metrics have improved as these are closely aligned to contact center efficiency. Moreover, managers no longer have to worry about planning for outbound capacity to handle an overflow of alert notifications as the centrally managed process takes care of this outbound calling on a global level.

Customer relationships too are benefiting from the improved notification process. Customers tend to have a more positive view of the bank knowing that the bank is able to approach them with personalized proactive notifications and quickly get them to agents focused specifically on identify theft.

looking ahead

With the ongoing success of the fraud notification project, the universal proactive notification platform is being leveraged by other bank initiatives. For example, to address congested ACD queues, the bank is able to offer callers the option to be automatically called back once an agent is available. The bank's collection process has also significantly improved as collection agents no longer spend an average of 45 seconds dialing and leaving messages on answer machines.

To further improve their relationship with customers, the bank is also starting to take advantage of the *Subscription Manager* module of Nuance Notification Hub. This web interface empowers customers to effectively become their own fraud specialists. Customers can define for themselves the fraud alert threshold amounts for each of their bank cards and to specify when and how they may be contacted through the day.

about Nuance Communications, Inc.

Nuance is in the business of helping companies better support, communicate with and understand their customers while maintaining operational efficiency goals. Nuance currently supports over 8 billion care interactions around the world. No other company has as much experience as Nuance in understanding how customers interface with a care operation. Our vision is to make every customer interaction a winning experience. For more information about our customer interaction solutions, business consulting and professional services, please visit www.nuance.com/care.