PRODUCT DATA SHEET

GENESYS

Genesys Fraud Management

Cloud-based proactive communications accelerate credit card fraud resolution

Benefits

- Quickly identify suspicious card transactions
- Alert cardholders via their preferred channels
- Confirm fraud by automated customer interactions
- Limit agent conversations to confirmed fraud cases
- Reduce fraud losses
- Minimize card usage disruption
- Improve customer loyalty

"Credit card fraud cost banks and retailers more than $11 billion in the United States, up 15%."

Bloomberg BusinessWeek

The Genesys Fraud Management solution is a proactive, interactive, multichannel communications solution. It enables financial institutions to uncover, alert, and resolve suspicious credit and debit card transactions in a highly efficient and effective way. The Genesys cloud-based Fraud Management solution integrates with fraud detection systems to offer real-time, personalized, and interactive dialogs, enabling financial institutions to automate fraud alerts and cardholder confirmations so that they can resolve cases in less time, thereby saving money, and increasing customer satisfaction and loyalty.

The value of receiving real-time interactive fraud alerts

Time is of the essence when it comes to fraud mitigation. With the Genesys Fraud Management solution, notifications are sent automatically to alert customers regarding potentially fraudulent card transactions, account access, or changes personal account information such as their log-in, password, email address or Social Security number. Financial institutions that capitalize on proactive alerts will suffer lower fraud costs and their customers will appreciate the touchpoints, which will increase customer satisfaction and the overall customer experience. Institutions that fail to do so, do a disservice not only to customers who see the value of alerts, but also to their own bottom line.

Consumers prefer to be contacted via multiple channels when fraudulent activity is suspected

Understanding how to best reach your customer is the key to an effective customer experience. Today's customers are increasingly mobile and difficult to reach through just one communications channel. An overwhelming majority of customers prefer to be notified by multiple and various forms of communication, and most are eager to indicate the type of alerts they receive and their preferred delivery method including a phone call, text message, and email, if fraudulent activity is ever suspected on their debit or credit cards. An effective multichannel alert escalation strategy that honors cardholder communications preferences is crucial in situations where time is of the essence and minutes wasted can cost financial institutions millions of dollars annually.

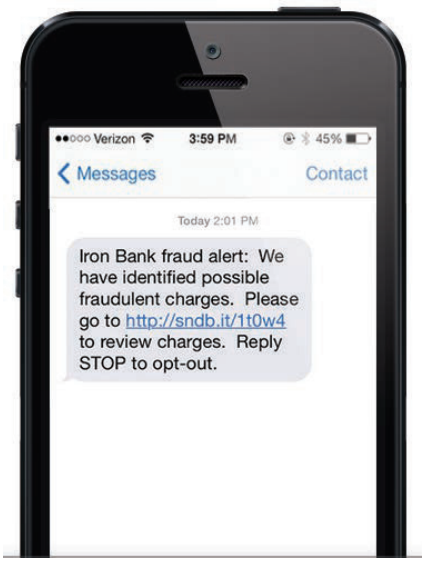

Figure: Multichannel communication preferences

Consumers prefer to be contacted via multiple channels when fraudulent activity is suspected.

Solution specifications

Real-time Fraud Detection Engine provides the connection point(s) to the financial service's case management system, fraud detection system, and/or system of record. The Fraud module triggers automated messaging to the cardholder when potentially fraudulent events are detected and coordinates the results of the cardholder interaction with real-time updates to the bank's system of record.

Campaign Strategy Manager enables banks to develop and manage notification decision-making strategies. Each strategy can be designed based on variables including time of day, fraud type, urgency level, transaction type, consumer communication preference, risk level, open to buy amount, and response outcome.

Cross-channel fraud alert escalation enables the coordinated use of multiple communications channels as part of the fraud notification strategy. For example, an initial alert could be sent via text message, and if not responded to within one hour, outreach expanded to an automated voice call.

Dialog Engine enables self-service and agent-assisted case resolution. It supports an interactive automated dialog initiated from an inbound or outbound cardholder message. Using its multi-channel rules engine, a bank can determine how to respond to a cardholder using pre-defined messages.

Contact and preference management functionality captures and augments cardholder contact information and lets account holders choose the type of alerts they receive and their preferred delivery method (phone call, text message, email). Build, manage, and maintain a database of customers to proactively communicate during the fraud management lifecycle via their preferred communication channels.

Reporting and analytics capabilities offer a variety of pre-defined and custom reports to measure and optimize the effectiveness of your communications strategies. Banks can easily tie results back to measurable business value including trends and data that identify how many fraud cases are confirmed without involving an agent, the best time to reach a cardholder, and how many cases are identified as true fraud.

Features

- Triggers fraud notification when suspicious activity detected
- Integrates with fraud detection systems, including TSYS CardGuard
- Customize contact strategies based on customer risk, business rules, and channel preferences
- Escalate alerts acros across multiple channels, including outbound IVR, dialer, SMS and email
- Enable self-service and agent-assisted resolution
- Capture and maintain cardholder communication preferences
- Update bank if cardholder confirms transaction is valid
- Transfer fraud victims to fraud specialist agent