Genesys

# State of Fraud Today

## Using Proactive, Real-Time Interactive Notifications to Fight Fraud and Increase Customer Loyalty

TABLE OF CONTENTS



## Rate of Fraud Incidents Continues to Increase

With identity theft and consumer fraud rising, and more frequent and sizable data breaches in the news, consumers need more protection than ever. The 2014 Javelin Strategy & Research Study[1] reported 13.1 million victims of identity fraud in the United States during 2013, or one victim every two seconds.

Financial institutions that take a multi-channel approach in fighting fraud can reduce fraud losses, in addition to maintaining customer loyalty and satisfaction. Proactive financial alerts, quickly give customers the necessary information and the tools to help combat fraud. Mobile plays a critical role by enabling you to effectively reach customers at any time and regardless of their location via interactive voice response (IVR), or text (SMS) alerts. Leveraging proactive alerts and multi-channel communications can help minimize the fraud costs faced by your financial institution.

## Consumer Fraud Impacts Financial Institutions

While overall fraud amounts increased in 2013, detection times continued to fall. The average victim suffered a loss of $4,930 in 2012, according to U.S. Department of Justice and Javelin Research. That leaves financial institutions to absorb the majority of fraud costs to limit the impact on customers. Javelin's 2013 Banking Identity Safety Scorecard[2] reported that banks continue to excel in resolution capabilities, with all top 25 banks surveyed offering zero-liability protection for signature, PIN, and card-not-present transactions for debit cards. A significant positive correlation continues to exist between the length of detection times and average customer costs. The longer fraud goes undetected, the higher the average cost to the customer — and to the financial institution. Costs to the customer are classified as any out-of-pocket expenses paid by the fraud victim, including unreimbursed monetary losses, lost wages while trying to resolve fraud, and any related legal expenses.

[1]Javelin Strategy & Research, 2014 IDENTITY FRAUD REPORT: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends, February 2014
[2]Javelin Strategy & Research, 2013 IDENTITY FRAUD REPORT: Changing Tactics in the Face of Growing Account Takeover and New Account Fraud, February 2013

**Identity Fraud Definition:** the unauthorized use of another person's personal information to achieve illicit financial gain. Identity fraud can range from using a stolen payment card account, to making a fraudulent purchase, to taking control of existing accounts or opening new accounts, including mobile phone or utility services.

- Javelin Research, 2014 Identity Fraud Report

Customers who took six or more months to detect fraud suffered more than 14 times the cost of those who discovered fraud in one day or less ($1,648 vs. $116), and nearly five times the average customer cost ($552). However, the increase in average costs for customers who take up to five months to detect fraud might be attributed to the following:

1) Financial institutions are not legally required to restore lost funds if customers fail to report the fraud within a certain period, and

2) Fraud that goes undetected for long periods tends to be more complex and more difficult to resolve.

## The Importance of Proactive Fraud Resolution

The growth in fraud is harmful not only because of dollars lost, but also because of the emotional impact on the affected customers. Victimization generates fear and a loss of confidence in existing organizations, leading many customers to avoid certain merchants, alter their use of payment types and channels, and sever relationships altogether. Eighteen percent of those victimized by fraud switch credit card companies, 17 percent switch primary banks or credit unions, and 31 percent switch forms of payment.

As customers become accustomed to, and come to expect, real-time financial information, the demand for multi-channel communication will be a necessity. Mobile devices in particular will enable customers to know where they stand financially anytime, anyplace — and to take action using the cost-effective banking channels they consider most practical, be it SMS messaging, email, voice, or going into a banking location.

To maintain the loyalty of customers effected by fraud, your financial institution must resolve fraud as quickly as possible, position itself as the customer's ally, and implement systems to satisfy new and existing customers. Taking such an approach will increase customer satisfaction and minimize attrition.

### Customers Desire To Be Contacted Through Various Channels

While banks and card issuers typically assume responsibility for fraud losses, there is an opportunity to partner with customers to build relationships and reduce costs. Control means confidence. Deputize your customers in the battle against fraud using a multi-channel communications approach to reduce fraud losses, lower customer service costs and boost customer loyalty. In essence, the mobile device can serve as a financial remote control that delivers the right information at the right time — and more and more customers will define "the right time" to mean in "real time". If you deliver such an experience, you will be the first place customers will turn to when monitoring and managing their finances.

Not all breaches are created equal. The study found consumers who had their Social Security number compromised in a data breach were five times more likely to be a fraud victim than an average consumer.

-Javelin Research, 2013 Identity Fraud Report

### Customers Want to Share Responsibility for Fraud Protection

When customers are asked how they would first like to be contacted regarding potential fraudulent activity on their account, it becomes clear that different customers prefer different means of communication. Because of the growing smartphone market and the increasing customer base with advanced mobile functionality, your financial institution must continue to develop mobile communications that will reach your customers through all available and desired channels.

When successful, fraudsters are now more than three times as likely to use the money stolen to buy prepaid or gift cards to make fraudulent purchases.

-Javelin Research, 2014 Identity Fraud Report

# The Value of Real-time, Multi-channel Interactions

Proactive financial alerts have the potential to initiate timely, practical and actionable conversations between you and your customers, delivering unprecedented control to customers over how they monitor and manage their money. Each alert is a personal exchange with a customer and can build trust by sharing control with customers and bolstering their confidence that their money is in good hands. In addition, by automating alerts, you have the ability to address incidents in a more timely and cost-effective manner. It is not always necessary for there to be direct contact between a customer service representative and the customer.

## Customers Highly Value Alerts

Financial alerts are also an effective way to involve the customer in fraud mitigation. Notifications sent automatically signal customers regarding potentially fraudulent changes to their accounts, or to their personally-identifiable information such as their log-in, password, email address or Social Security number.

Capitalize on alert offerings and partner with your customers to combat fraud to suffer lower fraud costs, increase customer touchpoints and enhance customer satisfaction. Failing to do so does a disservice not only to customers, who see the value of alerts, but also to your bottom line. According to Javelin, more than 50 percent of victims in 2012 were actively detecting fraud using financial alerts, credit monitoring or identity protection services and by monitoring their accounts. This activity has a direct correlation with the decrease in misuse time for all types of fraud including credit cards, loans, bank accounts, mobile phone bills and other types of fraud due to customer and industry action.

# Effective Communications Alert Offerings

Alerts are most effective when they deliver relevant information at the right time, when information is of peak value. As mobile banking and m-commerce gain momentum, serving up real-time transaction and account data will become increasingly important:

- Timely alerts can deputize customers in the fight against fraud, enlisting their help in spotting suspicious transactions.
- Implementing multi-channel alerts enables customers to take action in a channel most convenient to them. For example, customers could reply via text or IVR yes or no to a fraud alert to confirm whether a purchase was valid, or push-to-dial a customer service representative or interactive voice response system.
- Interactive alerts provide the ability to resolve customer concerns via automated messaging and providing customers with self-service options, without taking up more costly, traditional contact center agent resources.
- Alerts have the potential to open conversations, regardless of whether they typically bank online, via mobile, use ATMs, or prefer to walk into a branch. SMS text message and email alerts are able to reach customers who have turned off landlines or prefer to be contacted via their mobile devices.

Perhaps most importantly, alerts can demonstrate to customers that their financial providers are looking out for them 24/7, giving them greater control of their account.

The use of voice, text, email, and web channels means more interactions are resolved through self-service channels, resulting in cost savings and potentially freeing up resources for other fraud-fighting initiatives. It also underscores that alerts are most valuable and practical — and most beneficial to you — when they enable customers to quickly and easily take action in the channel the customer considers most efficient.

## Conclusion

By encouraging customers to enroll in email and mobile alerts as well as other monitoring programs, you can leverage the customer's willingness to help detect fraud sooner. Working with a cloud provider who can provide real-time fraud notifications while honoring a customer's preference and offering interactive mobile messaging delivers information that can minimize fraud damages, allow fast interaction, and increases customers loyalty and experience.

## About The Genesys Fraud Solution

The Genesys Fraud Management solution is a proactive, interactive, multi-channel 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 is integrated with TSYS CardGuard℠, to offer real-time, personalized, and interactive dialogs, enabling financial institutions to contact cardholders and resolve cases in less time, thereby saving money, and increasing customer satisfaction and customer loyalty.

**About Genesys**

Genesys is a leading provider of customer service and contact center solutions. With more than 3,000 customers in 80 countries, Genesys software directs more than 100 million interactions every day from the contact center to the back office, helping companies deliver fast, simple service and a highly personalized cross-channel customer experience. Genesys software also optimizes processes and the performance of customer-facing employees across the enterprise.

For more information visit: www.genesys.com, or call +1 888 GENESYS.

Corporate Headquarters 2001 Junipero Serra Blvd., Daly City, CA 94014 USA
Tel: +1 650 466 1100 | Fax: +1 650 466 1260 | www.genesys.com