Arresting Fraud with Automated Notifications

Using automated Fraud Alert Notifications to reduce exposure and increase customer satisfaction.

A Premiere Global Services Whitepaper

Premiere Global Services

Introduction

Identity theft and fraud cost consumers and financial institutions billions of dollars annually. Due to consumer protections, financial institutions bear the majority of the financial impact of fraud. For consumers victimized by identity theft and fraud, the financial costs are often overshadowed by the burdens of damaged credit history and the effort needed to repair it.

Early detection is one of the keys to minimizing the damage to both financial institutions and their customers. Automated notifications can alert customers to potential fraud indicated by irregular usage patterns or unusually costly transactions. With this information customers can detect and take actions to stop identity theft and fraud much sooner than if they learned about it through their credit card statements or calls from a collection agency.

Automated alerts can positively affect companies' performance and efficiencies in the following ways:

- Alerting customers of potential fraud for early detection and intervention.
- Reducing losses that must be written off by stopping fraud faster.
- Increasing customer satisfaction and longevity with proactive communications that help customers protect themselves.

Stolen: Billions of Dollars

In 2005, the Federal Trade Commission (FTC) received over 685,000 consumer fraud and identity theft complaints. Consumers reported losing over $680 million in these claims. But the true extent of these losses far exceeds what has been reported to the FTC. Studies by Javelin Strategy and Research, the Federal Trade Commission, and Gartner estimate the number of cases of identity theft and fraud is nearly 7-10 million every year, costing individuals and businesses billions of dollars.

Costs to Financial Institutions

Business Bears the Brunt

In 2005, losses to businesses from identity theft accounted for over 93 percent of the $56.6 billion in total losses.

- Javelin Strategy and Research

While the personal cost to the consumer can be great, financial institutions, such as banks, credit card issuers and processors, bear the majority of the financial costs of identity theft and fraud. In most cases, financial institutions can't hold their customers responsible for the costs of identity fraud, or if they do, only for a nominal amount, such as $50, with the bank footing the rest of the bill.

As a result, financial institutions suffer most of the financial burden for identity theft. The actual cost to business is difficult to measure, but the direct costs have been estimated to be around $50 billion per year. A Javelin Strategy and Research survey in 2006 reported that losses to businesses for the previous year totaled over 93 percent of the $56.6 billion in total losses from identity theft. These are only the costs for stolen funds that must be written off, and these costs don't take into account other costs, such as trying to recover the stolen funds.

Costs to the Consumer

On average, ID-theft victims are hit with $500 in personal expenses and take 30 hours to resolve issues, according to the Federal Trade Commission survey. This time can translate into lost wages and time

away from friends and family. Worse still, consumers may spend years trying to repair the damage done to their credit even after the case has been solved.

Doing a Disservice

According to a survey of victims of identity theft, less than 20 percent were pleased with the service they received from financial institutions and credit card issuers.

- Identity Theft Resource Center

While up to a third of victims of identity theft lost no money, the costs to consumers are much more personal. Victims of identity theft often feel emotions similar to that of victims of violent crimes. This emotional response can translate to a negative reaction toward their financial institution. The Identity Theft Resource Center surveyed victims of identity theft and found that less than 20 percent of identity theft victims surveyed were pleased with the level of service they received from their financial institutions and credit card issuers.

Early Detection is the Key

Early detection is the key to minimizing the damage caused by fraud to both financial institutions and consumers. Findings from the FTC survey show the following:

- When cases of identity theft were discovered in six months or more, thieves stole more than $5,000 44 percent of the time; however, when cases were discovered in five months or less, that number drops to 18 percent.

- When cases of identity theft were discovered within a month, thieves were able to open new accounts only 10 percent of the time.

Identity theft is most often caught by the consumer who is the victim. Often, the first time consumers learn about identity theft is when they get a call from a collection agency regarding charges they never made or accounts they never opened.

Consumers are encouraged to monitor their bank and credit card statements every month and check their credit reports at least once a year. Still, even the most vigilant consumer won't detect that they're the

victim of identity theft or fraud using these methods until weeks or months after the fraud occurs. More proactive ways to better detect fraud enable consumers to minimize the damage. One way to encourage early detection is through proactive Fraud Alerts to consumers.

What are Fraud Alerts?

One of the best ways to keep consumers aware of what's happening to their accounts is through fraud alerts. Fraud alerts allow companies to automatically contact customers, using voice or SMS, when out-of-the-ordinary transactions occur on their account. For instance, a bank could generate a fraud alert every time a transaction greater than $500 is performed using a customer's credit card. A fraud alert notification might say, "Mr. Smith, a $500 charge occurred on your credit card on May 3. If you did not perform this transaction, press 1 now."

An alert like this is minimally invasive to the customer if he did perform the transaction. If the customer did not perform the transaction, he has a jump-start on recovering from the fraud because he does not have to wait until he receives a bank statement or checks his credit report.

Forrester Research has identified three types of notifications that customers would like their financial institutions to provide:

- **Preemptive alerts** – Warn customers of possible issues so that they can take action to solve a problem or avoid a fee. Examples include alerting customers of insufficient funds in a checking account or that the account balance is about to fall below the minimum requirement.

- **Account-based alerts** – Help customers monitor transactions in their accounts, such as when deposits are made or a specific check has cleared, allowing them to draw on funds and ensure mailed deposits have not been stolen or misapplied.

- **Purchase alerts** – Keep consumers up-to-date when they are in the process of applying for credit or renewing a service, including notifications on the status of a loan application or a CD maturity notice. Purchase alerts can also be used to flag transactions that exceed a certain pre-set limit, such as any credit card purchases over $500, so they can be confirmed.

Fraud alerts can be customizable to the needs of any financial institution. For instance, if a bank has an automatic fraud detection system, the bank could notify customers whenever the fraud detection system finds a suspicious transaction. Or banks could allow their customers to determine a dollar amount over which they must first approve any charges to their account.

Fraud alerts give consumers more information and control over their accounts. Consumers are a financial institution's first line of defense when it comes to detecting fraud.

How Fraud Alerts Protect Financial Institutions

Fraud Alerts Work

One credit card issuer used an automated fraud alert service to increase fraud detection by 100 percent in six months.

- The Business, November 2004

Since financial institutions bear most of the cost of identity theft and fraud, early detection cuts down on the costs to the financial institution. In November 2004, *The Business* reported that one credit card issuer used an automated fraud alert service to increase fraud detection by 100 percent in six months.

A single undetected case of identity theft has the potential to cost your financial institution thousands of dollars or more, and the longer a case goes undetected, the more the case may end up costing. A single phone call, email, or SMS notification can save thousands of dollars in potential losses.

Additionally, fraud alert notifications can help your financial institution comply with new laws requiring that you notify customers of potential security breaches regarding customer information. And automated fraud

alerts are far less expensive than other costly methods, such as live callers or paper mailings.

How Fraud Alerts Protect Consumers

Value for Consumers

Of consumers surveyed:

73 percent highly value email alerts relating unusual transactions.

72 percent want the ability to receive immediate electronic alerts of suspicious transactions.

- Research and Markets

For consumers, receiving proactive notification from their financial institution adds value to their relationship with the financial institution. Consumers prefer to deal with organizations they can trust. If they are able to stop identity theft in its early stages or even to catch the culprit responsible with the help of fraud alert notifications from their financial institution, that organization establishes a powerful bond with their customer.

A 2005 Research and Markets survey found the following:

- 73 percent of consumers surveyed highly value email alerts relating unusual bank account transactions.
- 72 percent of consumers surveyed want the ability to receive immediate electronic alerts of suspicious transactions in a credit or debit card account.

Increasingly, consumers will expect their financial institutions to be able to provide automated fraud alerts. The surveys by the FTC and Javelin already recommend that consumers use alerts and notifications from their banks and credit card companies to protect themselves from identity theft.

Features to Look For

With a variety of options for automated notifications on the market, it is important to choose a solution with a set of features that match your company's needs. Some important features to look for include:

- **Customization** – With customizable notifications, you enter personal information for each call, such as the customer's name and information about the transaction causing the alert. Your customized notification might say: "[Customer Name], a [Transaction Value] charge occurred on your credit card on [Date]. If you did not perform this transaction, press 1 now." A text-to-speech solution can read the name and transaction information from your database.

- **Multiple Communications Channels/Modes** – Reach your customers anywhere, in the method that's most convenient for them, whether that's through voice, email, text messaging (SMS) or fax.

- **Interactive** – With interactive notifications, you capture a response from the customer. Using a key press or voice recognition, the customer can approve or deny a suspect transaction.

    - Email notifications can include links to view a statement or list of recent transactions to review and confirm activity.

    - SMS notifications can allow a consumer to reply and immediately approve a transaction or suspend an account.

    - Voice notifications can provide the ability to transfer to a live representative for more information or to provide specific instructions.

- **Hot Key Transfer** – A hot key transfers the customer, either through a key press or voice recognition, to a live customer service agent at any time during the call. With hot key transfer, if customers have questions about their account, they can speak to an agent for immediate resolution.

- **Reporting** – Full web-based reporting allows you to determine how effective your notifications are in reaching your customers and getting responses. You can determine which messages were

delivered, which messages were responded to, and which customers may need to be contacted again through a different channel.

Choosing a Provider

When choosing a notifications provider, it is important to find a provider with a proven track record in the notifications industry and with the highest capacity and reliability.

The Gartner Group suggests the following guidelines for choosing a notifications provider:

- The provider should have expertise in your industry. This is especially important in regulated industries like banking.
- The provider's tools should be easy for your company's planning and recovery teams to learn.
- The provider should supply training, technical support, and consulting services.
- The provider should have the ability to export data into and out of its product suite and enterprise applications so that administration of the tool is faster and less prone to error.
- The provider should offer a family of products that enable the tool to be upgraded easily as the plan grows.

Benefits of a Hosted Solution

The high cost of entry and difficulty in integrating with existing financial, database, and fraud detection applications may be a barrier to entry when implementing a solution on site. A solution hosted by an application service provider (ASP), however, can get you up and running

quickly at a fraction of the cost. Hosted services provide the following benefits:

- **Ease of Implementation** – A hosted solution resides offsite and is accessed through the Internet so you don't have to dedicate IT resources to setting up new infrastructure. Hosted solutions are designed to integrate easily with your existing systems.

- **No Need to Maintain** – The ASP upgrades software and provides routine maintenance on the platform, freeing you from support activities.

- **No Up-front Capital Costs** – You don't spend thousands of dollars up front on new hardware and software licenses.

- **Scalability** – The hosted provider is prepared to handle large volumes of notifications, so you will be prepared for the growth of your company or unexpected spikes in volume.

- **Value** – Rather than having to spend money on a system providing more capacity than you need, you pay for only the services you use.

Premiere Global's Fraud Alert Solution

Premiere Global Services' Fraud Alerts offer an easy-to-use, customizable fraud alert notification system. Financial institutions simply use their existing systems to upload a list of active notifications to Premiere Global Services. Premiere contacts each customer on the list, using the customer's preferred contact method, and records the results of the contact for the financial institution. Customers can even transfer directly to a live operator to take further action on the notification. Premiere offers a hosted solution, which means there is no equipment to buy. You only pay when you use the system, and volume-based pricing means that you get great value no matter how many notifications you need to send.

Summary

Identity theft and fraud costs businesses and individuals billions of dollars every year. One of the keys to reducing that cost is through early detection. Fraud alert notifications, such as those provided by Premiere Global Services, offer financial institutions a simple, cost-effective way to notify their customers of potential fraud, irregular account activity, and to approve unusually high charges. Fraud alert notifications give customers a sense of control over their transactions that means an improved business relationship with your bank, and the ability to immediately detect fraud can save both your customers and your financial institution thousands of dollars for every instance of identity theft cut short.

Resources

"Cavion Plus adds DigitalMailer's e-LERT service to eCommerce offerings." DigitalMailer 9 May 2005: Press Releases.

Federal Trade Commission. *Consumer Fraud and Identity Theft Complaint Data: January-December 2005*. January 2006. http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf

Gartner Group. "Gartner Says Identity Theft Is Up Nearly 80 Percent." July 2003. http://www.gartner.com/5_about/press_releases/pr21july2003a.jsp

Identity Theft Resource Center. *Identity Theft – The Aftermath 2003*. Summer 2003. http://www.idtheftcenter.org/idaftermath.pdf

Javelin Strategy and Research. *2006 Identity Fraud Survey Report*. January 2006.

Mearian, Lucas. "Disaster Notification Tools Get a Boost." Computerworld 15 Aug. 2005: Security/Disaster Recovery.

Synovate. *Federal Trade Commission – Identity Theft Survey Report 2003*. September 2003. http://www.ftc.gov/os/2003/09/synovatereport.pdf

About Premiere Global Services, Inc.

Premiere Global Services, Inc. (formerly Ptek Holdings, Inc.) provides business communications services and business process solutions that enable enterprise customers to automate and simplify components of their critical business processes and to communicate more effectively with their constituents. We offer data management and delivery solutions and conferencing and collaboration services on an outsource-basis, hosted on our global proprietary platforms. Customers apply our communication technologies-based solutions to a number of business processes, such as receivables collections, continuing education, alerts & notifications, investor calls, statement and invoice delivery, international collaboration, document automation, and other applications, in order to increase efficiency, to improve productivity and to raise customer satisfaction levels. With 2,230 employees in 19 countries around the world, Premiere Global Services℠ has an established customer base of approximately 60,000 corporate accounts, including a majority of the Fortune 500. Our corporate headquarters is located at 3399 Peachtree Road NE, Suite 700, Atlanta, GA 30326. Additional information can be found at www.premiereglobal.com.

0406

