



# Hire Your Customers to Detect Fraud

Empowering Your Cardholders to Address Fraudulent Card Activity  
in Real Time Can Better Serve Your Customers and Reduce Your Costs



Presented By

**PaymentsSource**  
Data, news and analysis for payments professionals

## ABSTRACT

A new solution from SoundBite Communications, Inc. brings credit and debit cardholders into the process of identifying and resolving card fraud. When a suspicious transaction occurs, an automated solution from the Bedford, Mass.-based company notifies the cardholder immediately, authenticates the cardholder's identity, asks if the transaction was legitimate, and then informs the card-issuing bank of the cardholder's response.

The SoundBite Fraud Management Solution contacts the cardholder by voice, text, email or a combination of those channels. The cardholder could receive the communication as a call, email or text message on a mobile phone, an email to a computer, or a call on a telephone landline.

Cardholders benefit because the solution contacts them the way they want to be contacted and immediately brings them into the fraud detection process. The card-issuing bank benefits because the automated solution reduces contact center costs, accelerates fraud resolution, and limits the banks risk of exposure to further losses.

This paper provides information on card fraud and how interactive multi-channel communications can help card-issuing banks address the problem of resolving card fraud effectively, while reducing expenses and building customer loyalty.

## CARD INDUSTRY OVERVIEW

**Worldwide, the top card issuers are handling 99 billion credit and debit card transactions annually.** The U.S. accounts for more than half of those exchanges of value, topping 56.4 billion transactions each year.<sup>1</sup>

**To stay at the pinnacle, Americans have increased their use of cards 24 percent since 2003.** Some 576.4 million credit cards and 507 million debit cards were in circulation in the U.S. by the end of 2009,<sup>2</sup> and the average American cardholder had 3.5 cards by the end of 2008.<sup>3</sup>

**Identity fraud costs Americans an estimated \$54 billion annually and continues to grow as debit and credit card transactions increase.** In fact, more than 11 million U.S. residents fell victim to the crime in 2009, up from 10 million a year earlier. One contributing factor to the increase, the careless use of social-networking sites, willingly exposes personal data to the prying eyes of criminals.<sup>4</sup>

**Meanwhile, in England and Wales, victims of card fraud recently increased 40 percent in a single year to more than 2.4 million.** Credit and debit card fraud, which cost the United Kingdom's banks £440 million last year, is rising quickly even though fears of a recession-induced crime wave have failed to materialize.<sup>5</sup> At the same time, card fraud has become three times more likely than burglary in UK, and 6.4 percent of UK cardholders fell victim to fraud in 2008-2009, up from 4.7 percent the previous year.<sup>6</sup>

<sup>1</sup>The Nilson Report, February 2010

<sup>2</sup>The Nilson Report, February 2010

<sup>3</sup>Federal Reserve Bank of Boston, The Survey of Consumer Payment Choice, January 2010

<sup>4</sup>Javelin Strategy & Research, 2010 Identity Fraud Survey Report, February 2010

<sup>5</sup>British Home Office, 2009 British Crime Survey

<sup>6</sup>British Home Office, 2009 British Crime Survey

## WHAT BANKS REQUIRE

Because banks offer consumers zero-liability protection, financial institutions are absorbing the loss of funds stolen through card fraud. With the increase in card fraud, issuing banks need to reduce their exposure to risk and accelerate fraud resolution at a lower cost. Relying solely on cardholders to find fraud on statements takes longer and costs for the card-issuing banks can soar.

Banks are challenged to resolve fraud earlier while managing customer experience, costs and process. Early detection enables banks to prevent additional transactions, thus limiting further liability.

**1. Identify Fraud Quickly:** When a card issuer's fraud-detection system or case management system flags unusual transactions, the institution often has no real means of determining whether the anomaly constitutes fraud. In many cases, only the cardholder can declare a transaction legitimate or fraudulent. To obtain that cardholder's judgment as quickly as possible, the bank needs a communications strategy with the most effective outreach.

**2. Achieve Cost Effectiveness:** Automated one-way communications that alert cardholders to the possibility of fraud but do not establish an interactive dialog can increase the number of inbound calls that tie up agents and thus increase expenses. Cardholders need an automated channel to confirm the transaction is not fraudulent. If the case is fraudulent, the solution should quickly connect the cardholder to a fraud specialist to resolve the matter. Such a solution frees agents from addressing lower-risk transactions, so they can concentrate on addressing true fraud.

**3. Contact More Potential Victims:** Having contact center agents manually contact possible fraud victims is time-consuming and can drive up costs. As a result, card-issuing banks that rely on agents to contact cardholders personally are forced by economic considerations to limit their attempts to only the cases most likely to have resulted from fraud.

**4. Increase Customer Contact Points:** Banks face a challenge in finding the right ways to proactively reach cardholders at any given moment. Out-dated or missing customer contact data makes it difficult to proactively notify cardholders when suspicious activity has been detected, or if a card has been blocked. The consumer may not know the card has been blocked until attempting a transaction, giving rise to frustration and dampening customer loyalty.

**5. Faster Response Rates:** Consumers have high expectations for customer service but can be difficult to reach and are increasingly "on the go". If a card issuer understands the best way to reach the cardholder, and has that contact information, it will resolve fraud faster. Issuers need a solution that can reach the cardholder on their mobile devices through the preferred communications channels to ensure quick responses and faster fraud resolution.

**6. Minimize Card Usage Disruption:** Bringing cardholders into the fraud-detection process gives consumers greater control of their finances. When banks ask cardholders to verify unusual transactions they build trust and customer loyalty. In cases that do involve fraud, cardholders know why their cards have been deactivated and are not caught unaware and inconvenienced at the point of sale.

---

## CARDHOLDERS DO NOT WANT TO LEARN THE HARD WAY

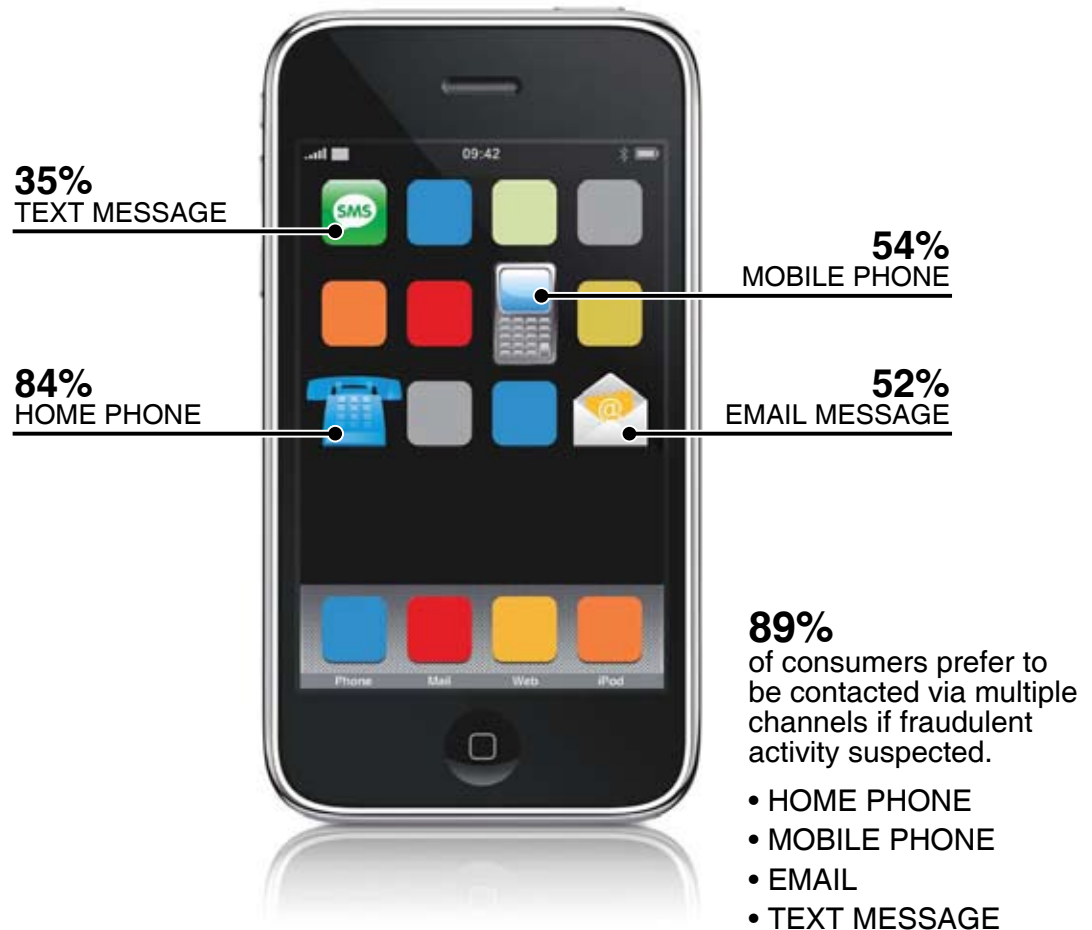
Cardholders who are asked to verify fraud keep abreast of what is happening instead of finding out after the fact. They appreciate that inclusion, but attempts to contact them count for little unless the bank's systems succeed at the task. Successful contact requires using the preferred communications channels selected by the consumer. To do so, banks must have a solution in place to solicit and update cardholder contact information proactively.

Banks can begin to understand the importance of choosing the right channels of communication with the help of a study SoundBite recently commissioned.

### MULTI-CHANNEL COMMUNICATIONS IS KEY

Card-issuing banks can address the burgeoning threat of identity theft by using automated two-way communications to alert cardholders to suspicious account activity. Effectively communicating the threat of fraud plays an integral role in customer relationship management and loyalty.

Consumer communications preferences vary widely and many consumers prefer to be contacted through more than one communications channel. An overwhelming majority of consumers — **89 percent** — prefer their financial institutions notify them of potential fraud through multiple forms of communication, including phone calls, text messages and email. That finding arose from the Fraud Cardholder Communications Survey; a telephone canvass of 1,017 respondents aged 18 or above, conducted by Harris Interactive in March 2010 on behalf of SoundBite Communications, Inc.



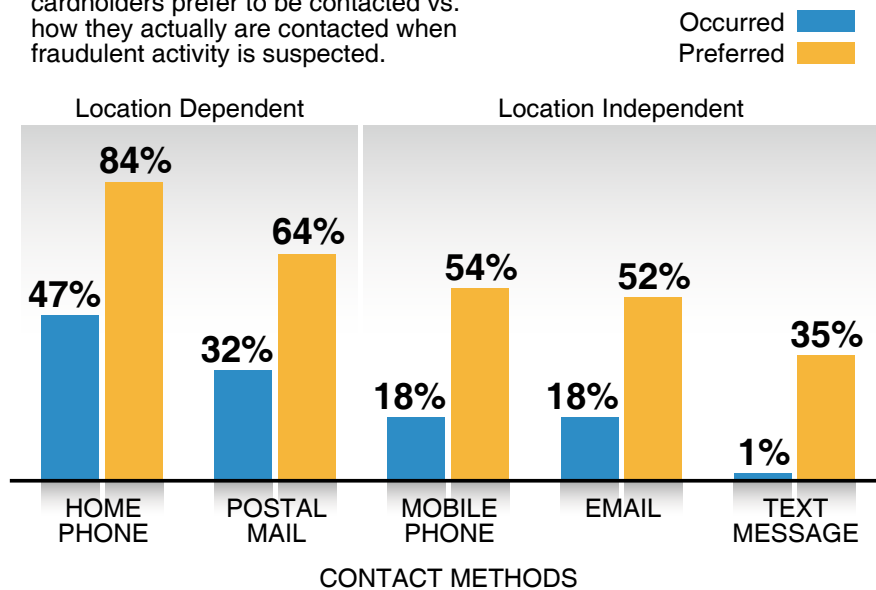
## CONSUMER DISCONNECT: WHY DIDN'T YOU TEXT ME?

The cost of fraud increases dramatically the longer it takes to resolve suspicious card activity. Contacting cardholders and validating transactions quickly are critical to stemming further losses. Effective communications require that banks understand their cardholders' communications preferences and have a mechanism for honoring those preferences.

Card-issuing banks need to consider how cardholders want to be contacted when fraudulent activity is suspected, the survey indicates. Thirty-five percent of consumers surveyed indicated they would like to receive notification by text message, yet only one percent of those in that age group who have been fraud victims were notified that way, according to the recent survey. Understanding these communications preferences facilitates a faster response from the cardholder. As the survey also found that the primary way a bank could improve the customer experience during this critical time, was to know the best way to reach the cardholder.

Traditional communications channels, including the home phone and postal mail, are dependent on the individual being present in that location. To successfully interact with a cardholder, time-sensitive communications must honor both the cardholder's communications preferences and the trend for more location-independent communication modes. With more than half the global population now using mobile phones, communication strategies must include mobile communication channels such as email, text, and calling mobile phones.

There is a disconnect between how cardholders prefer to be contacted vs. how they actually are contacted when fraudulent activity is suspected.



## THE SOUNDBITE FRAUD MANAGEMENT SOLUTION

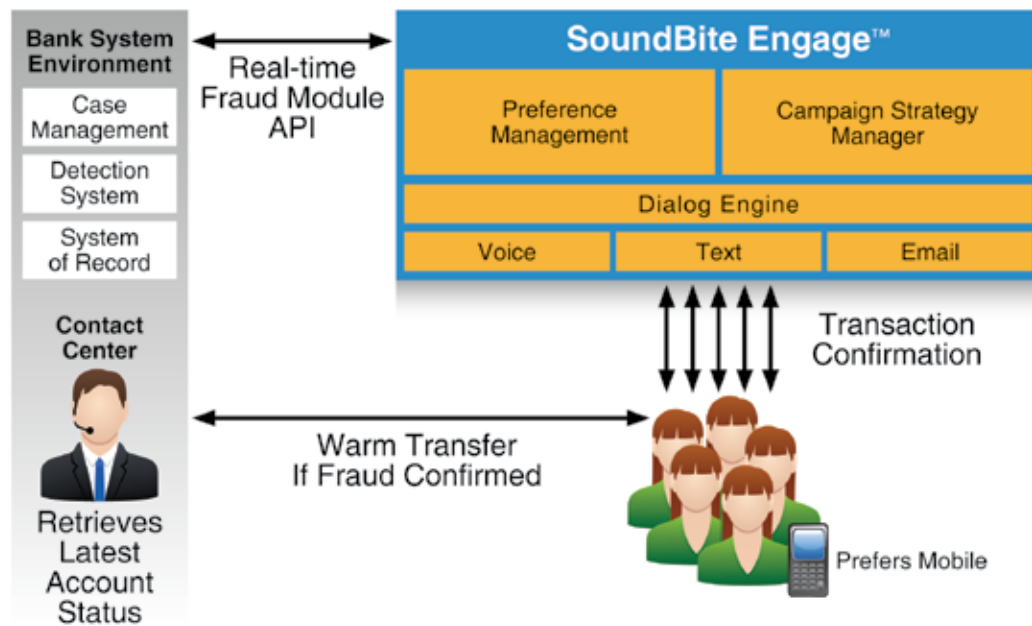
Looking at what banks require and what consumers want, SoundBite packaged an effective approach to communicating with consumers when a financial institution has reason to suspect fraud. SoundBite's Fraud Management Solution is an interactive, multi-channel cardholder communications solution.

Enabled by SoundBite Engage™, a multi-channel, proactive customer communications platform, the Fraud Management Solution integrates with fraud detection systems, including TSYS CardGuard™, to trigger personalized, interactive dialogs so that banks can contact more cardholders and resolve more cases in less time. This provides banks with an efficient and effective way to alert, uncover, and resolve the growing number of suspicious credit and debit card transactions.

"The new solution brings credit and debit cardholders into the process of detecting fraud," says Colleen Ayres, senior product marketing manager, SoundBite Communications. When a suspicious card transaction occurs, SoundBite's solution immediately notifies the cardholder, authenticates the cardholder's identity, asks if the transaction was legitimate, and then informs the card-issuing bank of the cardholder's response.

## HOW THE FRAUD MANAGEMENT SOLUTION WORKS

The solution helps banks enhance their contact strategy by understanding cardholders' preferred communications channels. The solution immediately contacts cardholders using interactive, personalized communications across voice, text, and email communications channels to resolve suspicious account activity as quickly as possible.



**1. Bank Detects Suspicious Activity:** Communication is triggered when the rules engine of the card-issuing bank's fraud-detection system discovers purchases or withdrawals that do not fit the cardholder's established patterns. When a deviation occurs, the bank's systems evaluate the level of risk and take action.

**2. Real-Time Fraud Module Receives Cardholder Information:** Fraud notifications occur almost instantaneously. "Once the bank detects suspicious activity and alerts SoundBite, we can notify in minutes," says Ayres. A cardholder making an unusual purchase online, for example, might receive an email message concerning the transaction before getting up from the computer.

**3. Consults Preference Management:** The solution can optimize its contact strategy using the cardholder's preferred communications channels. One might not have a telephone landline for example, and prefers to receive text messages and email.

**4. Executes Multi-Channel Campaign Strategy:** If the solution cannot reach the cardholder on one channel, it tries to make contact through another. "The bank may initiate contact to you through a phone call and if it doesn't reach you at home, it could automatically escalate to a text message and email," Ayres says.

The solution reinforces the message by communicating through multiple channels. If the system reaches the cardholder by phone, for example, it can send a text messaging confirming that the transaction was resolved which may prevent an inbound call to the contact center. "Some consumers might be comforted by written confirmation and won't feel the need to confirm the transaction with a contact center agent," says Ayres

**5. Triggers Personalized Cardholder Interactions:** The fraud management solution integrates tightly with a card-issuing bank's internal fraud detection systems so that the automated dialog can begin between the bank and cardholder.

That integration with the issuing bank's systems also enables the solution to use the cardholder's personal information to verify the person receiving the communication is the right recipient. To that end, the SoundBite solution conducts an automated dialog that may ask for personal data such as the cardholder's mother's maiden name, billing ZIP code, high school, or other qualifying data.

Once the bank and cardholder establish their identities, the solution provides details of the fraudulent transaction, possibly including the amount of the transaction or when and where the transaction occurred, depending on the bank's communication strategy.

**6. Resolves Case and Updates Bank:** The cardholder then indicates whether the transaction was legitimate, and the solution relays the outcome of the dialog to the card-issuing bank.

Cardholders who indicate a transaction was fraudulent are transferred into the card-issuing bank's contact center to speak with a fraud specialist. The information gathered during the initial proactive notification, including details provided by the cardholder, appears on the fraud specialist's computer screen.

"The fraud specialist is prepared for that conversation," says Ayres. In cases of fraud, the bank can halt further transactions on a compromised account.

When the cardholder confirms the transaction as valid, the communication is completed in the automated mode. SoundBite relays this information to the bank. The bank then updates its case record and prevents future fraud communications concerning this transaction.



## **BUILDING CARDHOLDER LOYALTY**

Handling the notification and follow-up properly inspires confidence among cardholders. “It’s an opportunity for the bank to increase customer loyalty,” Ayres says. “It can be a scary time,” she points out. “So being proactive and communicating in a way that the cardholder feels good about can deepen the cardholder’s trust in the card-issuing bank.”

The elements of the process combine to instill consumer loyalty by “deputizing” cardholders and putting them in charge, Ayres notes. In fact, one out of three cardholders feels more loyal after an incident if the bank handles the episode properly, she says. Banks, besides reaping the benefits of increased loyalty, gain the advantages of addressing fraud quickly, reducing costs and limiting exposure, Ayres continues. “Everybody wins,” she says.

---

## **DOMAIN EXPERTISE**

SoundBite Communications, Inc. (NASDAQ: SDBT) is leading provider of on-demand, multi-channel Proactive Customer Communications, which enable organizations to communicate relevant and timely information to their customers over a variety of communications channels. Seven of the 10 largest card-issuing banks, as well as 50 Fortune 500 companies in several industries rely on SoundBite to proactively communicate with their customers.

The 10-year-old Bedford, Mass.-based company offers interactive Customer Lifecycle Solutions that address key business challenges to help businesses build strong customer relationships from acquisition through retention. In the case of card-issuing banks, the lifecycle would begin with origination, continue with card activation, and follow through with loyalty, payments, fraud management and collections. The company’s Optimization Solutions provide enterprise-wide solutions that enable more efficient and effective customer interactions. Both are powered by SoundBite Engage™, the company’s on-demand, multi-channel communications platform. For more information visit [SoundBite.com](http://SoundBite.com).