Fraud-busting

IN THE DIGITAL ERA

How retail banks can fight back against consumer and employee fraud

ttec™

Combatting Modern-Day Financial Fraud

All employees should be able to recognize the red flags of fraud.

Financial fraud isn't new, but technology has ushered in even more pervasive forms of fraud. Thieves are using increasingly sophisticated means and refining their approaches to steal valuable data.

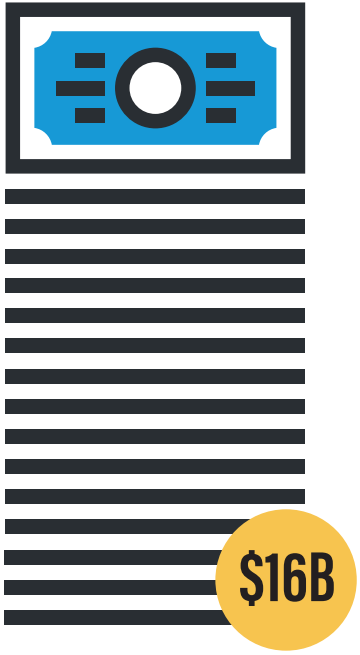
Still, there are steps banks can take to limit their vulnerability. Well-informed and trained employees are the first line of defense against fraud.

This e-book outlines fraud trends and how to help employees proactively combat them, includes a case study, and highlights fraud-busting technology trends.

TABLE OF CONTENTS

The High Costs of Fraud

Thieves stole nearly $16 billion last year and fraud cases continue to rise.



Last year, about **15.4 million consumers** were victims of fraud, up from 13.1 million in 2015, with fraud losses totaling $16 billion.

About **1 in every 16** U.S. adults were victims of ID theft in 2016 and the incidence rate jumped about 16% year-over-year.

Card-not-present fraud rose **40%** last year.

Account takeovers — where a criminal steals credentials for an existing account — climbed **31%**.

Instances where thieves open new accounts in someone else's name are up, too, by **20%**.

For every dollar a merchant loses to a financial scam, it typically incurs **$2.40** in fees, chargebacks, and merchandise replacement.

What to Look For

Fraud can take many forms, but the attacks against retail banks and other financial institutions can generally be described under the following categories:

Cybercrime – Online theft committed on a financial institution's internet or computer networks.

Mobile Banking Fraud – Smartphones and mobile banking applications are increasingly becoming targets for fraudsters. Hackers will target the information on the device, as well as the information the device can access and the messages it receives.

New account fraud – Creation of a new account by an unauthorized person.

Account takeover – Gaining unauthorized access to an existing account.

Debit or credit card fraud – Unauthorized use of credit or debit card information in order to steal funds.

Identity fraud – Stealing an individual's personal and/or financial information for financial gain.

Check fraud – Illegally using checks (either by the account holder or an unauthorized individual) for financial gain.

Employees: Fraud's Best Defense

Employees play an important role in preventing fraud. Here are several best practices for helping employees detect illegal activities.

Educate associates on how to recognize fraud techniques such as phishing attacks and emotional appeals.

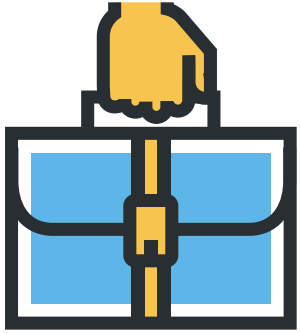
Use real-time monitoring solutions to track historical voice data and call content for suspicious signs of fraud. The solution can then alert associates to the presence of a suspicious caller.

Train associates to perform basic internal audits outside of their daily tasks to provide oversight.

Conduct penetration testing periodically to ensure security protection is maintained across the platform.

Guarding Against Employee Theft and Fraud

Unfortunately, employees can also be a source of fraud. Banks can reduce the chances of employees committing fraud themselves with the following tips:



Use an IVR system to validate spoken or keyed credit card numbers from customers. This way the associate never hears the card number or the touch-tones used to enter the card number.

Especially for small businesses, **make sure duties are separated** with checks and balances built in. Allowing an individual to control many services is asking for trouble.

Train managers to watch for changes in an employee's behavior. If files have been misplaced, a customer receives excessive attention, the employee is suddenly working longer hours, etc. look into it.

Ensure security patches/updates are installed in end-points and enforce them.

Spotlight on Remote Employees

There are many benefits to hiring remote contact center associates: They can provide support during off-peak hours and high-volume seasons, and flexible schedules appeal to higher quality employees.

Effective security measures are necessary with remote employees.

Train remote associates to never access the contact center over public Wi-Fi (restrict or develop instant notifications if they do) and provide an SSL VPN for logging into the center.

Use technology to require remote associates to activate and update antivirus software on any computer used to access the contact center.

If using a bring-your-own-device model, use a technology solution that prevents the sharing of work/customer data and personal PC data.

PC administrator access should never be granted to home-based workers, and applications should be delivered through a virtual desktop instead of installed locally on the PC.

5 Ways to Proactively Fight Fraud

In addition to employee-focused data security, there are measures, that when implemented collectively, can greatly reduce a company's vulnerabilities to fraud.

1 Create a centralized fraud prevention strategy

Many fraud prevention programs are not integrated into the company's broader risk management framework. Instead, a fraud team may conduct one-off risk assessments without getting an accurate view of the overall risk landscape. A better approach is to combine departmental data to build models that can estimate the true probability of an attack and make informed decisions on how to address it.

2 Implement multi-factor authentication controls

Multiple authentication controls such as biometrics (e.g., fingerprints and voice recognition), temporary PINs, and text message verification can make it difficult for thieves to impersonate account holders. Additionally, firms should implement behavioral authentication, which uses algorithms to detect abnormal behavior like unusual IP addresses and multiple failed login attempts.

.

3 Conduct frequent fraud assessments

Companies must conduct comprehensive fraud risk assessments regularly. However, only about 50 percent of firms perform fraud risk assessments at least annually, according to PwC. When assessing risks, companies are advised to use data analytics to prioritize and maximize the effectiveness of the fraud monitoring program.

4 Make fraud awareness and training a requirement

Fraud prevention efforts are only as strong as the weakest link. All employees, especially front-line employees and customer service specialists, should be knowledgeable about fraud threats and red flags. Employees must also know what to do when a fraud attack occurs and what steps to take to contain it.

5 Create a zero-tolerance culture for insider threats

Companies must also guard against internal fraud. In addition to conducting background checks on employees and providing a fraud hotline, it's incumbent on companies to maintain a culture of internal accountability and awareness of the consequences of committing fraud.

.

CASE STUDY

Bank Enables Safe and Efficient International Fund Transfers

Challenge: A large U.S. bank wanted to improve the quality of fund transfers from U.S. accounts to Mexican accounts, while improving the overall fund transfers process. U.S-based associates lacked sufficient knowledge and training of the bank's systems and the Spanish language to properly assist customers. This increased handle time and lowered customer service scores for U.S.-based associates. Also, the solution utilized by the client did not prevent fraudulent transactions.

Solution: We created special systems training and workforce management strategies to enable more efficient call handling, in addition to hiring more Spanish-speaking associates based in Guadalajara, Mexico. To address fraud concerns, we implemented additional verification processes in the money transfer process and analyzed customer account information to identify uncharacteristic transactions. We also implemented additional reporting to track transactions at an associate level and limited associate ability to perform transactions without a customer on the phone.

RESULTS

75%

drop in fraud instances, from 200 per month to 50

60 seconds

difference in handle time for our associates compared to internal bank associates

The Future of Fraud-busting

Four predictions about trends that will mark the next wave of fraud prevention.

Machine learning will become an important part of fraud detection and prevention solutions. Applying machine learning to decision-scoring, for examples, increases the speed and accuracy of security safeguards and authentication processes.

Natural language analytics identify narrative patterns that are characteristic of fraud. Instead of just flagging keywords, natural language analytics will be used to flag suspicious messages on email, text messages, social media, etc.

Voice-biometrics software will be able to identify emotional patterns that may indicate deceit.

Advanced lie-detection techniques such as **analyzing facial expressions** or screening for certain **pheromones associated with stress** will flag non-verbal irregularities of an interaction.

About TTEC

TTEC (NASDAQ: TTEC) is a leading global provider of customer experience, engagement, growth and trust and safety solutions delivered through its proprietary end-to-end Humanify™ Customer Engagement as a Service offering. Founded in 1982, the Company helps its clients acquire, retain, and grow profitable customer relationships. Using customer-centric strategy, technology, processes and operations, TTEC partners with business leadership across marketing, sales and customer care to design and deliver a simple, more human customer experience across every interaction channel. TTEC's 49,500 employees live by a set of customer-focused values that guide relationships with clients, their customers, and each other. To learn more about how TTEC is bringing humanity to the customer experience, visit ttec.com.

ttec™

 70609 11-17