Four Ways To Help Your Customers Fight Fraud

cyber security digital banking fraud protection

Summary: Are you doing everything you can to help your customers fight fraud? We share four ways that your peers are doing this, including text messages, locking and unlocking cards, and education.

Denmark has 2x the number of bicycles as cars and almost every road has a bike lane. Unfortunately, the abundance of bikes leads to an opportunity for thieves — 17% of Danes have stolen a bike at some point.

Similarly, thieves abound in the banking world. Community financial institutions (CFIs) continuously develop ways to fight fraud internally, but their efforts can be greatly enhanced if they also offer resources for customers to detect possible fraudulent activity or attempted social engineering scams. We found four ways that CFIs are helping their customers fight fraud. Likely, you are doing most of these already, but, these important reminders can start the year off right.

1. **Fraud text alerts.** Many CFIs send text notifications to customers' mobile phones if and when suspicious transactions occur on their debit or credit cards. Customers reply to texts to verify or dispute transactions. The institutions let customers know that the alerts will always display the CFI's name and text number, and will never ask for any personal or account information – just questions that require only "yes" or "no" answers. Customers with additional questions are encouraged to call the institution for more information.
2. **Unlocking and locking cards.** Some institutions offer customers the ability to lock the use of their debit or credit card online or in the mobile app, if they believe someone else has the card. Customers also have the ability to unlock their card, when it's safe to do so. If they see a suspicious charge themselves, customers can click on the transaction online or in the mobile app and follow links to report a problem and immediately start the process of getting their money back.
3. **Fraud prevention education for individuals, including seniors.** Many CFIs have fraud prevention education webpages for customers. The information explains how criminals can use their personal information to access their bank accounts, obtain loans, make purchases, rent an apartment in their name, get medical services, or otherwise use the customer's identity for their own purposes. CFIs give customers directions on what to do if they suspect identity theft and how to repair it. CFIs send updates to customers about different types of social engineering scams on emails and social media sites too. They also educate seniors with tailored alerts of scams that specifically affect them.
4. **Fraud prevention recommendations for commercial customers.** Some CFIs have fraud prevention education webpages for business customers too. They recommend: internal security enhancements for employees and accounts; validation controls to help stop attempted payments fraud on checks, wires, and ACH payments, along with behavior monitoring of all outgoing ACH wires transactions, wire transfers, and other online banking activity. CFIs also provide business customers with advice about adding fraud-related riders to their business insurance policy, including riders covering cybercrime, fraudulent bank transfers, and employee dishonesty or embezzlement.

THREE TIERS TO FIT YOUR CECL NEEDS

CECL is one of the biggest challenges these days. CECL FIT gives you options to fit your portfolio with a web-based intuitive solution, including as little or as much expert assistance needed. Plus, we include a 100%

cancellation guarantee. Learn more about our CECL solution.