TREASURY MANAGEMENT

PROTECTING AGAINST FRAUD:
A CHECKLIST OF CONSIDERATIONS FOR YOUR ORGANIZATION

Be sure that you are protecting your company from fraud by following proven best practices, diligently monitoring accounts for fraudulent activity, and reporting to your bank in a timely manner to increase the likelihood of recovering funds.

Some of these best practices may be obvious, but they make a good checklist for your internal fraud mitigation efforts.

- **Take advantage of the controls available in your card technology platform.** For example:
  - **Credit limits:** Avoid making more funds available on an account than are needed to support that cardholder. Make sure that any temporary limit increases that are needed revert back to normal levels quickly and automatically.
  - **MCC Code and volume restrictions:** Use MCC codes to restrict the kind of activity that can occur on an account and set limits on the size of the transaction or the number of daily transactions or amount that can occur on the account. This strategy can help stop a fraudster who's gotten their hands on an account number and is trying to quickly wreak as much havoc as possible.
- **Use a central travel account or a virtual travel program** to minimize the credit limit on individual cardholders' accounts. Large dollar expenses, like airfare and hotel, are billed to a central account with these solutions.
- **Close accounts that aren't being used.** Store active cards securely. And avoid having the program administrator activate cards on behalf of the cardholder.
- **Don't write the PIN on the card.** If you're using chip and PIN cards, keep the PIN secure and change the PIN by calling the number on the back of the card if you think the PIN may have been compromised.
- **Verify the identity of individuals who call program administrators.** Fraudsters can social engineer their way into finding out administrators' names. The fraudster might call the administrator and ask for a reminder of their security code. When processing a request by phone, administrators should verify the identity of the cardholder.
- **Avoid using simplistic codes that could be easily guessed as your security code**, like 1111 or sequential digits. Also avoid using personal information that is publicly available. If the fraudster knows your name and can discover your birth year, for example, or the last four digits of your SSN, they may be able to pose as you.

Chip-on-chip transactions now represent almost 64% of the U.S. payment volume. That's nearly 2 billion U.S. Visa® chip transactions, representing 73% of payment volume.

This transition has resulted in an 80% decrease in counterfeit fraud with chip-enabled merchants.

However, fraud is migrating to less-protected channels. Fraudsters are aware that they can't counterfeit physical cards and use them in a chip environment anymore. As the online environment is less protected, card-not-present fraud is growing.*

*GBI data for the month of December 2018. Visa-branded transactions processed as chip transactions.

PNC®

- **Don't use a common security code for all cardholders.** Provide each cardholder with a unique code and, if possible, avoid using personal information.
- **Don't use the same card number for multiple employees.** Transactions could be declined if the card numbers are used at the same time in two different locations. Even more important, if there is a fraudulent transaction, you can't really tell who performed the transaction if multiple people are using the same account.
- **Implement a usage policy and communicate that in your organization.** Monitor it and update it regularly for your cardholders so that you're able to report fraud in a timely manner.
- **Enroll in your provider's liability waiver program and follow the required protocols.** If there's internal fraud occurring on the account, having a cardholder agreement in place and terminating the offender of the fraud can be highly effective in limiting your risk.

In addition to the processes and tools used to detect fraud, the industry continues to develop products and solutions that can minimize the instances and impact of fraud. Your bank should also offer comprehensive fraud mitigation products and services.

READY TO HELP

PNC focuses on helping you balance fraud reduction with the cardholder experience and often can work with you to help you develop fraud strategies for your specific situation. For more information, contact your Treasury Management Officer or visit **pnc.com/treasury**.

CIB TM PDF 0519-0168-1261901