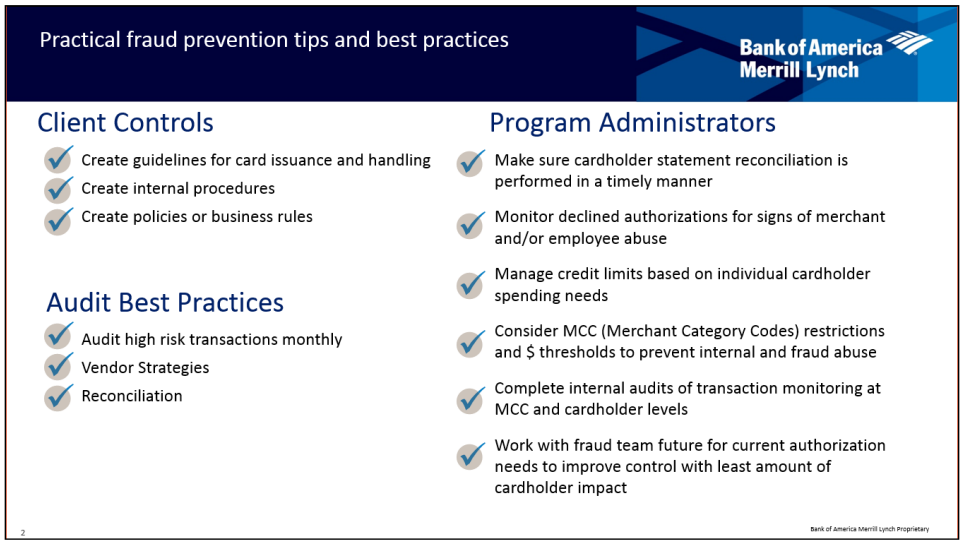
Fraud Prevention Best Practices for Corporate Card Program Managers

Welcome to a Bank of America Merrill Lynch Podcast, *Fraud Prevention Best Practices for Corporate Card Program Managers.* I'm Kevin O'Hanlon, Senior Product Manager for Global Card and Comprehensive Payables at Bank of America Merrill Lynch.

In this podcast, we'll talk about fraud prevention and fraud management strategies for commercial card program managers, including some practical tips and best practices for securing your card program.



Fraud Prevention Best Practices for Corporate Card Program Managers

Bank of America Merrill Lynch

When we speak of **client controls**, the first thing we want to talk about is creating guidelines for card issuance and handling. The most important thing that we recommend is that you segregate your duties from whoever is ordering the cards versus whoever is receiving the cards. And we can't stress enough that you should have a minimum of two program administrators.

Think about it from a perspective of how you manage your strategic payments. You have one person prepare it; you have another approve it and send it. It's a check and balance arrangement. The program administrator role within a commercial card program is very powerful. You have a lot of visibility. You have self-administration tools. You can change credit limits. So in addition to the auditors reviewing all of the actions that take place, you want to, at a minimum, have two people involved in the process of ordering and issuing new cards.

The second recommendation from a control perspective is to **determine who should be able to apply for a card**. It has to deliver a benefit to your organization, and remember, you do have to manage and control this. You don't want to just issue a card to everyone in your organization.

We also recommend that you determine the approval levels required. Who has to say 'yes', and depending on whether they say 'yes', what should the card limits that you set up be for that particular individual?

When we move to **internal procedures** that you create, we recommend that there be requirements for obtaining a card. So within your organization, consider factors such as the individual's frequency of travel or their job function. If you're going to be issuing cards to your Purchasing Department, consider which types of purchases can go on a card and which purchases are restricted.

Likewise, within your accounts payable and accounting requirements, you want to make sure items are coded appropriately when they are reconciled. You should determine when the documentation needs to be submitted, and the frequency and timeliness of reconciliation. Reconciliation is critical because this is where your cardholder will identify potential fraud. And, it's commonly known that you have no liability for fraud and fraudulent transactions as long as you report them to the bank in a timely manner.

Many times the bank will be the first to notify you about fraud. We'll let you know that something looks suspicious and alert you to fraud, but sometimes, you are the first line of defense to let us know that a card has been compromised and needs to be replaced.

Finally, from a **business rules perspective**, here are some of the key items that we recommend around fraud prevention.

The first is around the **use of cards** in your program. Will you allow personal transactions? Our overwhelming recommendation is that you only allow your program cards to be used for business transactions. Intermingling personal charges convolutes the reconciliation process as well as the data you have to manage your program, so we recommend that you do not allow personal use. We *do* recommend you have an exception process should someone make a mistake and use their card for personal purposes by accident.

Cash access is another consideration. You have to look at where you travel or use your card. If it's mostly domestic, we know that 98% of transactions can most likely go on your card, and incidentals for cash are typically related to things like tips. So if you are going to allow cash, we would recommend that you set a minimal threshold of the percentage of the cardholder's credit limit. Also, from an audit perspective, we would recommend that you test for high cash usage. Whenever you have high cash usage, it is an audit flag.

From a policies perspective, consider how you're going to deal with **card sharing.** Are you going to allow it? Because if it's a department card, you have to have policies around who utilizes the card, and what the reconciliation methods are. If you don't know who is using the card, it can create liability.

We recommend that you have **training** before a card is issued. Cardholders really are only looking for you to establish the rules and expectations, and they will meet your expectations, whether they're minimal or whether they are detailed. So we recommend you have a process in place where people review their responsibilities before you issue them a card.

And finally, from a business rule perspective, we recommend that you have a policy around **audit exceptions** out of the ordinary type of transactions around receipt thresholds or lost receipts. Once again, you want to make sure people know what to do when something happens that is not an ordinary transaction.

Let's discuss **audit best practices**, and what you should be auditing for. We recommend you focus on high-risk transactions monthly. This includes cardholders with the highest number of transactions and cardholders with the highest dollar amounts spent. Also, employees with multiple disputes are where we typically could see fraudulent activity.

We also recommend that, **as you issue new cards**, in the first 60 to 90 days, you should audit a sample of those new cardholders to see if they understood the policies, if they're doing it correctly. You want to catch it in the early days in terms of getting everybody to follow the policies that you put in place.

From a vendor perspective, you should be sure that you look at the number of vendors utilized and number of transactions per vendor. Negotiated vendors -- are they being utilized? And transactions between a cardholder and the same vendor.

From a **reconciliation perspective**, we would recommend that you look for split purchase occurrences that avoid a dollar threshold policy. You want to make sure that employees are following that threshold and not splitting a transaction to avoid it.

We also recommend you look at the **unique or unusual vendors**. Nowadays with systems such as PayPal or Square, pretty much anybody can be a vendor, so you're looking for some unique names that might not be common names that you would use in your program.

As we close, a few reminders for program administrators: The first is make sure your cardholder statement reconciliation is performed in a timely manner. You obviously want to make sure that you're paying for services rendered and goods received, but timely reconciliation is also the first client line of defense in identifying fraud. And second, you should **sign up for mobile alerts which** will notify you that a transaction has been declined due to potential fraud. If the transaction truly is fraud, it provides you the ability to contact our fraud department directly. However, if the transaction is not fraudulent, you can respond that the transaction is valid. This will remove any blocks and allow you to continue using your card without ever having to call the bank. You can also set up alerts with a threshold, for instance: "Notify me anytime there's a transaction over $100." And if you're not transacting and all of a sudden you get an alert from us that says, "Here's your most recent transaction," you know you've been compromised. So it's another avenue to give you real-time visibility as to what's happening with your card. We all do it in our consumer lives, and we recommend that we do it in our professional lives.

This concludes our podcast. We hope you found this information useful and will consider these best practices to protect your corporate card program.

Thank you for listening.

Notice to Recipient

Bank of America Merrill Lynch

"Bank of America Merrill Lynch" is the marketing name for the global banking and global markets businesses of Bank of America Corporation. Lending, derivatives, and other commercial banking activities are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Securities, capital markets, strategic advisory, and other investment banking activities are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, locally registered entities. Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.
This document is intended for information purposes only and does not constitute a binding commitment to enter into any type of transaction or business relationship as a consequence of any information contained herein. These materials have been prepared by one or more subsidiaries of Bank of America Corporation solely for the client or potential client to whom such materials are directly addressed and delivered (the "Company") in connection with an actual or potential business relationship and may not be used or relied upon for any purpose other than as specifically contemplated by a written agreement with us. We assume no obligation to update or otherwise revise these materials, which speak as of the date of this presentation (or another date, if so noted) and are subject to change without notice. Under no circumstances may a copy of this presentation be shown, copied, transmitted or otherwise given to any person other than your authorized representatives. Products and services that may be referenced in the accompanying materials may be provided through one or more affiliates of Bank of America, N.A.
We are required to obtain, verify and record certain information that identifies our clients, which information includes the name and address of the client and other information that will allow us to identify the client in accordance with the USA Patriot Act (Title III of Pub. L. 107-56, as amended (signed into law October 26, 2001)) and such other laws, rules and regulations.
We do not provide legal, compliance, tax or accounting advice.
For more information, including terms and conditions that apply to the service(s), please contact your Bank of America Merrill Lynch representative.
Investment Banking Affiliates are not banks. The securities and financial instruments sold, offered or recommended by Investment Banking Affiliates, including without limitation money market mutual funds, are not bank deposits, are not guaranteed by, and are not otherwise obligations of, any bank, thrift or other subsidiary of Bank of America Corporation (unless explicitly stated otherwise), and are not insured by the Federal Deposit Insurance Corporation ("FDIC") or any other governmental agency (unless explicitly stated otherwise).
This document is intended for information purposes only and does not constitute investment advice or a recommendation or an offer or solicitation, and is not the basis for any contract to purchase or sell any security or other instrument, or for Investment Banking Affiliates or banking affiliates to enter into or arrange any type of transaction as a consequent of any information contained herein.
With respect to investments in money market mutual funds, you should carefully consider a fund's investment objectives, risks, charges, and expenses before investing. Although money market mutual funds seek to preserve the value of your investment at $1.00 per share, it is possible to lose money by investing in money market mutual funds. The value of investments and the income derived from them may go down as well as up and you may not get back your original investment. The level of yield may be subject to fluctuation and is not guaranteed. Changes in rates of exchange between currencies may cause the value of investments to decrease or increase.
We have adopted policies and guidelines designed to preserve the independence of our research analysts. These policies prohibit employees from offering research coverage, a favorable research rating or a specific price target or offering to change a research rating or price target as consideration for or an inducement to obtain business or other compensation.
Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor. No information contained herein alters any existing contractual obligations between Bank of America and its clients

3