

Airbase Corporate Cards

Fraud Policy & FAQ

This document describes our policy related to fraudulent transactions on physical and virtual Airbase Corporate cards. It includes answers to the following frequently asked questions:

- [Why does your agreement say that we're liable for all fraudulent transactions?](#)
- [What do I do if I want to report a fraudulent transaction on a physical or virtual card?](#)
- [How does the chargeback process work?](#)
- [Does the chargeback process involve any fees or other restrictions?](#)
- [Does Airbase employ any fraud prevention measures?](#)

Why does your agreement say that we're liable for all fraudulent transactions?

Our agreement has two parts to it:

- **Airbase Services Agreement:** This is the agreement between Airbase and your company, and the terms we're mutually agreeing to before we work with each other.
- **Card Program Agreement:** This is the agreement that our bank partner who issues our physical and virtual cards requires all of our customers to agree to.

The language that says you are liable for fraudulent transactions is in our bank partner's agreement. Since they do not interact with every customer we onboard, but issue the cards, they do not want to be liable for any fraudulent transactions and are protecting themselves from any claims. They are basically making it clear that any fraud-related claims will be addressed by Airbase and not them. So, the language in our contract does not mean that there is no fraud protection and that you're liable for all fraud. See below for more details on how we handle fraud.

What do I do if I want to report a fraudulent transaction on a physical or virtual card?

If you suspect that a transaction is fraudulent, immediately lock the card while you investigate. This avoids more fraud. Once you're sure that a transaction is fraudulent, follow these steps:

- Suspend the card. This is an irreversible action and you'll have to issue a new card to the vendor (if it's a virtual card) or employee (if it's a physical card). Suspending a card that you know has been compromised is very important and Airbase will not be liable for any future fraudulent transactions on the card.
- Write to support@airbase.io and let us know that you'd like to request a chargeback process on the transaction.

How does the chargeback process work?

Once you ask us to initiate a chargeback, we'll work with our bank partner to get the process going. Visa makes the final decision on all chargeback requests since our cards are issued by them. It can take many weeks for a decision to be made. We follow up regularly to get updates for you so that you don't have to check in with us regularly, but feel free to do so if you haven't heard back from us after 6 weeks. We may also reach out to you for more information about the specific transaction.

The ultimate decision is about who is liable for the fraud — the merchant (the entity where the card was fraudulently used) or issuer (Airbase). If Visa decides that the merchant is liable, then you'll see a refund processed into your account on the same card. The money will be refunded even if the card has been suspended and your account balance will increase by the corresponding amount.

If the issuer is found to be liable, then either Airbase or you will be liable for the fraud. We follow a simple policy of treating our customers fairly and doing the right thing when we decide who is ultimately liable in this scenario. If there was nothing you could have done to avoid the fraudulent transaction(s), then we'll refund you. Examples include:

- A physical card is skimmed without your knowledge and later used fraudulently in a store.
- A vendor to whom you've provided a virtual card is breached and the card is used fraudulently.

There is not much you could have done to avoid the above scenarios and it's not really your fault, so we'll refund you.

But, if the fraud happened because of an avoidable scenario, then you will be liable for it. Examples include:

- You or your employees share card numbers via email, Slack or other insecure means (use our secure sharing feature instead).
- You don't report a lost or stolen card as soon as you find out and there are fraudulent transactions in the interim.
- You don't suspend a card after you notice fraudulent transactions on it, and then see more fraudulent transactions in the future.
- You don't suspend an employee's card after they leave the company and they continue to use it (we don't consider this to be fraud).

The bottom line is that we want to do right by our customers and will treat each instance of fraud in good faith. We want you to realize that preventing fraud is a shared responsibility. You and your team have an important part to play in it and you will likely be liable for any losses if you don't do that.

Does the chargeback process involve any fees or other restrictions?

Our bank partner has a restriction that they will not accept a chargeback request if the transaction amount is less than \$100. But, please let us know if you see a fraudulent transaction that's less than \$100 since it will help us improve our fraud prevention systems. We also routinely refund the amount, unless it happens often with your account.

The bank partner charges us a \$35 fee per chargeback request, which we pass on to our customers. Their motivation behind this is to avoid frivolous chargeback requests since there's a real cost to investigating and processing each request.

Does Airbase employ any fraud prevention measures?

Yes! We employ many fraud prevention measures. As is typical policy for fraud prevention systems, we can't talk about it in detail since it will reduce the effectiveness of the various approaches we use. Having said that, it's important to realize that fraud prevention is a cat and mouse game that never ends. It's not possible to completely eliminate fraud. We're always trying to find the right balance between the experience we deliver to cardholders and having enough controls in place to minimize fraud.

While traditional banks send an email / expect the cardholder to call the bank to have the card reactivated, Airbase empowers the employee to take quick action to move forward.

One example of that is when we decline a transaction that we suspect to be fraudulent, but ask the cardholder via email and mobile app notifications if they are trying to use the card at that moment. If they confirm, we let it through on the next try.

The perfect experience is to never put up any hurdles in front of a cardholder, and also to completely avoid fraud. No card issuer reaches that ideal state. But, we try hard to strike the right balance and we always appreciate feedback about how we're doing. Please write to us at support@airbase.io if you have feedback for us about how we're doing in this regard.