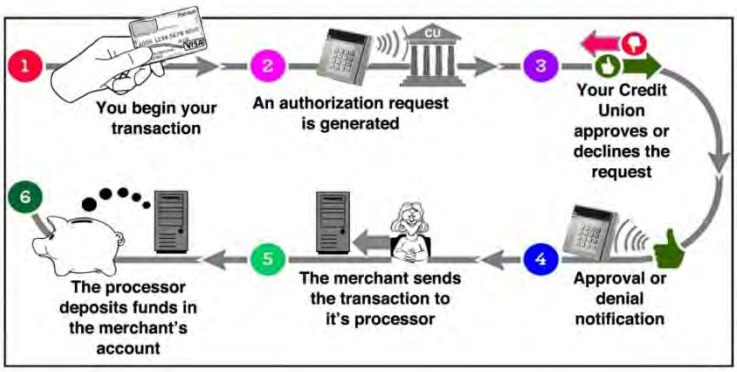
## Whose Fault Is Fraud? The Complicated Reality Of Debit Card Transactions

When you use your debit card, you visibly see an actual interaction between three people.

1.) You tell a **merchant** you'd like to buy something.

2.) That merchant tells your **credit union** to pay out some of your money.

3.) Your credit union asks **you** to authorize the transaction.




If something goes wrong in that process, it must be the fault of one of those people, right? The assumption is, either your credit union, the merchant or you gave out information that resulted in fraud.

Like most realities of the modern financial world, though, nothing is simple about your transaction. Let's take a look at three other places a financial transaction could break down, and what you can do to protect yourself.

**1.) The point-of-sale system**

Ever notice how most of the boxes that process credit and debit transactions look pretty similar? It turns out there are only a few companies that manufacture those systems. They're called **Point of Sale** (POS) terminals, and they're the lifeblood of many of today's small businesses.

The problem with anything made by so few manufacturers, though, is that anyone who learns how to defraud one of these terminals can do some serious damage. That was the weakness exploited in the Home Depot and Target hacks of 2014. These companies had one style of POS terminal for every store, so when a hacker group learned how to break into it, group members could steal data from a wide range of targets.

POS systems have a variety of other vulnerabilities, from PIN tracking keypads to miniature cameras. Always be on the lookout for small modifications in the keypads and other devices. If something looks suspicious, don't be afraid to back out of a transaction, or ask if there's another register you could use. Merchants are usually unaware of such rip-off efforts and will be grateful for alert customers.

**2.) The merchant's processor**

TIny margins are critical to most businesses, especially places that do a lot of transactions, such as gas stations, grocery stores and restaurants. To help keep costs low, these businesses turn to third-party payment processors. These companies take all the transactions a merchant has in a day, bill the appropriate entity (like a credit card issuer, such as a credit union), and pay the merchant. In exchange for this work, processors take a percentage of each transaction, usually less than 1 percent.

There's a great deal of competition in this niche, as companies continually offer lower prices to try to attract merchant business. This price competition also means processing companies are cutting costs, trying to stay profitable. One of the unfortunate ways in which they do so is by cutting corners with security.

Payment processing companies also deal with hundreds of thousands or even millions of transactions daily. When not all of these companies use industry-standard data safeguards, they represent another point in the chain where data security can be compromised. These processors represent a real risk of fraud.

When shopping at unfamiliar places, you can be extra-safe by using a pre-paid debit card, cash or another form of non-electronic payment. When in doubt, don't be afraid to visit an ATM and pay cash. ATMs are usually maintained by organizations with in-house processing, which limits the number of steps your data goes through. If you're working with a merchant you trust, you might ask who does their payment processing. Most of the big credit card companies have preferred providers who follow the highest quality payment processing procedures. A little research can help you find out if you should continue to take the highest precautions with that merchant.

**3.) Clearing houses**

The last stage in the payment processing chain is the clearing house. Large credit organizations, like major credit card companies, have external organizations that make the transfer of funds for them. They're the go-betweens for the merchant's payment processor and the credit organization.

There's a wide network of American Clearing House (ACH) payment centers. Most of them are entirely functional organizations that process millions of dollars worth of transactions every day without a hiccup. However, they are staffed by people. People occasionally make mistakes or have bad days, and some of those millions of transactions may be processed improperly. Fortunately, clearing houses are insured against losses, so they very quickly correct any mistakes they do make.

Every payment system has the possibility for fraud. A clerk could make change using phony bills. A check could be cashed multiple times. Goods can be counterfeit, or registers can overcharge. Electronic payment processing is among the most secure and convenient form of exchange possible, and its failures are public, but fixable. Use your debit card with confidence, knowing your liability is limited thanks to the strong paper trail protection offered by electronic payment processing.

**SOURCES*:**


http://gizmodo.com/home-depot-was-hit-by-the-same-hack-as-target-1631865043

https://www.firstdata.com/downloads/thought-leadership/where_security_fits.pdf

https://www.nacha.org/ach-network


This article is for you complements of MembersAlliance Credit Union.

Please feel free to share!

MembersAlliance CREDIT UNION
You can **rely** on us!

2550 S. Alpine Rd. Rockford, IL 61108 – Phone 815-226-2260

https://www.membersalliance.org/