Daisy **chain** is a financial **scam** conducted by a group of investors in the public equities market. These investors team up to increase the value of an equity security, and then flip their ownership of that equity to unsuspecting investors who are chasing an upward trend.

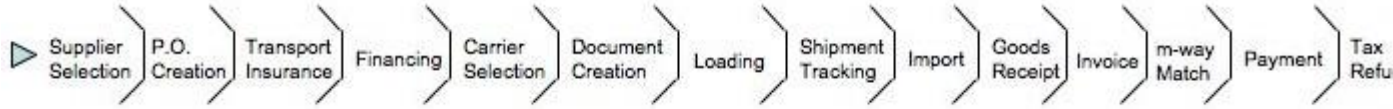
Fraud in the Supply Chain

As discussed in the last section, supply chain fraud is a rampant problem. More so than the bank-frauds that tend to get all of the news attention. The authors believe that this is likely due to a number of factors. Supply chains are bigger, and more complex, and present more opportunities for fraud. Businesses with complex supply chains employ more people than banks do, and it's a lot easier to get a job as a receiving clerk or a warehouse worker than it is to get a job as a hedge fund manager which requires degrees, certifications, and experience. Complex supply chains usually have lots of holes where fraud, if kept to a value that is small relative to the value of goods that flows through the chain (which often have a value in the hundreds of millions of dollars over the course of the year), can often be committed in a manner that will be undetected. There are lots of opportunity for repeat occurrences, and just like the former town official in Willimantic, Maine managed to embezzle funds for over 10 years before being caught, there could be individuals in your supply chain stealing from you on a daily basis and you might not know it.

Where It Can Happen

The simple answer is that it can happen everywhere. It can happen inside your four walls, inside the four walls of your manufacturer, inside the four walls of their raw material supplier, and at every touch-point and (especially) at every hand-off in between.

Let's start by examining the inbound supply chain, as described in the Global Trade wiki, and pictured below:



Fraud can occur at each step of the inbound supply chain. Some (common) examples of fraud that can occur at each step are:

Supplier Selection

- A supplier can submit a higher-quality product than it actually plans to, or is capable of, delivering in a bait-and-switch.
- A purchaser could select the vendor on the basis of a bribe or kickback.
- The supplier might not even be a real supplier, it might a shell corporation owned by the employee in an attempt to double bill for work done. (E.g. Your quality assurance manager contracts a third party review to a company he owns, and reviews the product himself on company time.)

card fraud scams

Best practices for mitigating fraud, safeguarding reputation and ensuring a good customer experience

The prevalence of fraud in the prepaid card space is low but persistent. Consumers rely on prepaid cards for a variety of reasons. They're confident of a card's safety because it's not tied to their personal information or banking. But the fact that prepaid cards aren't attached to a bank account actually means that customers who become fraud victims have no legal recourse and have particularly difficulty in uncovering the crime. Addressing fraud in this space helps ensure a good experience for the prepaid card customer and safeguards your organizational reputation.

Here are five popular prepaid card scams and some best practices for mitigating them:

Telephone scams: A fraudster calls into a merchant who sells GPR (general purpose reloadable) products. The fraudster says that he's calling from the mobile payment provider and needs to test the clerk’s terminal. When the clerk resists, the fraudster persists, saying that this is a necessary protocol that will get the clerk fired if he doesn’t comply. The clerk relents and gives the fraudster a pin number for a GPR, which the fraudster immediately loads into a card on his end and then cashes out at an ATM that he's standing beside. He tells the clerk that the signal from the store’s terminal is weak or distorted, and that they'll need to run the test again. This process happens three or four times until the fraudster has amassed $2000 to $3000. The fraudster hangs up and the clerk realizes that he's been scammed.

How to mitigate this scam – Training and velocity monitoring.

Card swaps: A fraudster enters a location with branded prepaid cards or GPRs that are hanging on racks in card packs. The fraudster steals the card packs, uses a razor blade to open a card pack and replaces the real card with a fake card. He then takes the card packs with the fake cards back to the location and waits for the fake cards to be activated. When they are activated, the fraudster redeems the funds from the cards.

How to mitigate this scam – Design a tamperless package and train clerks to detect this activity.

Packaging compromises: Fraudsters take a gift card or prepaid card from the rack and skim (copy the magnetic swipe data) from one card to another card and then wait for skimmed card to be activated. Once it is activated, they have an exact copy of the activated card. Skimming is very difficult to determine.

How to mitigate this scam – Redesign packaging so that the magnetic stripe cannot be accessed without destroying the packaging. Also, put the last four numbers of the card on the package and ensure the clerk compares those numbers to ensure the integrity of the card.

Method of tender: If you accept prepaid cards for payment, chances are you'll get stolen cards presented for payment.

How to mitigate this scam – Train your retailers on how to protect the card acceptance process at the point of sale by: 1) having the card present for the transaction, 2) getting a signature from the sales clerk, and 3) getting an electronic authorization. If the retailer completes these steps, even if the card is stolen, the retailer won't lose the money.

Tax fraud: Criminals complete tax returns using fraudulent identities and have the proceeds forwarded to their GPR card.

How to mitigate this scam – Match the name on the GPR account to the name on the IRS return.

Creating a frictionless experience for consumers is very important to organizational reputation. The final best practice is to step in very quickly to investigate and resolve any losses.

What is a phantom account?

Phantom Account is a form of guest **account** with limited permissions and it will be used as default system **account** until your device is marked recovered - preventing anyone from logging into other user **accounts** or accessing users data.
If the *Phantom Account* is created and you mark your device as missing, ESET Anti-Theft will block access to your active user accounts to protect your sensitive data. Anyone who attempts to use the device will only be permitted to use the Phantom account. Phantom Account is a form of guest account with limited permissions and it will be used as default system account until your device is marked recovered - preventing anyone from logging into other user accounts or accessing users data. The *Phantom Account* helps ESET Anti-Theft recover your lost or stolen computer by monitoring its location and usage.
You can enable the *Phantom Account* two ways:
•click **Create a Phantom account** in the **Optimization** tab of the ESET Anti-Theft web interface.
•click **Create** next to **Phantom account state** in the Settings tab of the ESET Anti-Theft web interface.