# Card Testing Attacks

Card testing attacks are among the more sophisticated frauds practiced by code-literate criminals in the digital space. Credit and debit cards can fall prey. They begin with acquiring data. The data could be a repository of card numbers and names stored in a spreadsheet, database, or anywhere vulnerable to hackers. The word *hacker* is a bit antiquated in the new digital age of organized larceny. We imagine the hacker as a loan operator in a dark windowless room with three computer screens in front of him — not to be sexist but Rami Malek patented the hacker image with *Mr. Robot* — when in reality it's more like a rented office space with numbers approximating a call center. It's the *Avante-Garde* of criminal fashion now — the adrenaline rush of robbery without the stigma of violence — a kind of white-collar Robin Hood zeitgeist, but beyond TV and movie spin is organized crime and state-sponsored economic warfare. North Korea comes to mind. There's nothing cool about data theft.

## How it Works

The purpose of the card test attack is to know whether a stolen credit or debit card is functional. Can it be used? Is there gas in the tank? Or has it been reported stolen and canceled? The testing is quite thorough. The data is qualified — name, associated accounts, expiry, balances — and this happens on differing scales. It can be one card or a batch of card data. If it's the latter it's more serious, a professional criminal ring with the ability to code and write scripts, capable of testing hundreds of cards against numerous online vendors, and they can do this very quickly, even simultaneously test the data of huge numbers of cards. Many of the actors in this criminal profession could go to the other side and work in cybersecurity. We don't want to put them on a pedestal, nor do we want to celebrate them, but in war, it's best to see your enemy as he is, and to give him realistic consideration, Sun Tzu, *The Art of War*.

### Act One: Get the Data

It all begins with getting the data, nothing fancy tried and true methods — if it isn't broken don't fix it — data breaches, small business owners cooperating with organized crime to read cards and save the read data, hacking databases to download stockpiles of credit and debit card information.

### Act Two: Validate the Data

Once a batch of data is acquired in the form of stolen credit card or debit card information, the criminal operators use software tools and scripting to test the stolen card data online. Imagine a robot playing a hundred slot machines at the same time over and over, waiting for the winning chimes on any number of machines. That’s how it works. A sophisticated criminal organization can run vast quantities of card numbers, expiry dates, and Card Verification Value (CVV) code combinations rapidly until they crack the cards and discard the invalidated cards, then another large batch is loaded into their system. It’s malfeasance at a manufacturing scale.

### Act Three: Small Purchases

In act three they have validated cards. This means the data associated with the cards is still valid and on record, however, our intrepid criminals don't know if there are security watches on the data, which can be conceptualized as bait lines to catch thieves. They then test the cards, small purchases to start, very innocuous. They study the circumstances to see if the card raises any alarms. Oftentimes the card can be reported stolen very soon after a data breach. This occupational hazard has to be addressed by the thieves. The method is low-volume transactions to begin.

## Digital Thieves Manage Their Risk

Top-tier digital bandits will go about their business with a certain level of risk management. They know what they're up against. They know what the security systems are monitoring. Smooth operators will spread their tests over numerous different accounts. They'll use proxy servers or IP spoofing to mask themselves or operate from compromised accounts. The thing you need to realize is how prepared these people are to steal. Their trade is illegal but they go about it with a surprising level of professionalism. They manage their risk.

A single successful transaction validates the stolen data. The card's good. They move to the next link in their criminal chain. They have options. The verified card can be sold through the dark web, or larger transactions can be made. They'll use the card and then throw it away, but not before they achieve their threshold of acceptable purchasing when measured against their risk. And they do measure their risk. The name of the game for them is staying out of jail, and not getting caught, and they can be very disciplined about managing their risk.

## Losses

The losses are felt by both the card data owner and the merchants that get scammed. The owner of the card data loses money. The merchant loses market reputation. The last thing a company wants is public knowledge of the fact that hackers scammed them out of products with fraudulent data and fraudulent cards. If you think the risk to reputation is exaggerated, all you have to do is recall the 2013 breach of Yahoo. It took five years to figure out how serious the breach was. It wasn't until 2017 that they admitted publicly that all three billion of their registered accounts were affected. It's hard to measure these things but it's safe to say Yahoo never quite recovered from that 2013 breach.

To fight back against card testing attacks both merchants and consumers have to participate. Security is a basic and necessary component of any online vendor now. The larger the vendor, the more money put into marketing the company name, and the larger the risk of reputational damage if they get taken by digital bandits. It's all dollars and cents. Bad public relations is like an inverse marketing budget. The marketing budget is worth nothing if the company's reputation suffers through persistent or intermittent losses that become public knowledge.

## Defense is the Offense

So how do you fight back? How do you defend yourself against card-testing attacks? There are several tried and true methods — transaction monitoring, velocity checks, captcha verification, IP location analysis, and fraud detection algorithms.

Many of them when combined with the power of machine learning (ML) and artificial intelligence (AI), say for example transaction monitoring, become exponentially more effective because of the efficiency of ML and AI, which is capable of much more pattern recognition detail in the monitoring of transactions. Machine learning implies that the machine is learning, so, at a certain point, it's going to start teaching itself how to become more adept at looking for anomalies in transaction monitoring. This technological innovation increases the security of merchants and cardholders. The old tools — two-factor authentication, address verification systems, card verification codes, and transaction velocity monitoring — are reformed and reinforced by ML and AI, like the legions of Greece coming to the aid of Leonidas and his 300 Spartans, and not a moment too soon, because the thieves are global, 24 hours a day, seven days a week.