FINANCIAL FRAUD consortium

BIN Attack Fraud

How can we work together to keep growth viable while continuing to provide best in class security and due diligence?

Compiled for the *Financial Fraud Consortium*
by Victoria Starr, CFCS

About the Financial Fraud Consortium

Mission

Stop Complex Fraud

To mobilize the consortiums' expertise to proactively detect, expose and mitigate fraud within all facets of the rapidly evolving payments industry

Members of the Financial Fraud Consortium fully understand that the evolving payments ecosystem is always at ever-increasing risk. As fraud increases in frequency and sophistication, collaboration plays a vital part in preventing, detecting, and responding to events to mitigate considerable financial losses or significant risk to reputation in the marketplace.

The Basics

BIN Attack fraud, also referred to as BIN testing, enumeration, brute force, or velocity attack fraud, is not a new methodology employed by perpetrators.

In fact, a BIN attack is a combination of fraud methods used to capture card data, validate that data, and in turn commit transactional fraud all on a very large scale with minimal manual effort for the perpetrator. Here are some of the basics integral to this fraud scheme.

What is a BIN?

The Bank Identification Number (BIN) is typically the first four to six numbers of a card number. It identifies the both the card network and the issuer of the card.

How is the fraud carried out?

Using a known BIN, in conjunction with number generating software, the perpetrator may derive a full card number (and often another verifying point such as expiration date or CVV). They employ a card testing scheme by submitting many *Card not Present* authorizations to validate the derived card data. Authorizations may include small dollar amounts for testing followed by larger dollar authorizations quickly depleting the card. Or the perpetrator may sell the successfully validated card data.

In recent years, some perpetrators have also used the same scheme but employed large scale authentication attempts to capture payment details from various online merchants.

Why is this profitable for the perpetrator?

It can be inferred that the attempts during the testing phase tend to produce mostly declines, so why would this be profitable for the fraudsters? Due to the possible scale and technological automation of the scheme a successful authorization (or authentication) rewards the perpetrator with a validated card they may use or sell, all with minimal effort, in a short period of time, and without much risk of being caught.

Who is the victim of a BIN Attack?

Unlike other consumer centric types of fraud, the victims in BIN Attacks tend to be those in the Payments business – Processors, Issuers, Merchants, Program Managers, and Networks.

Financial Fraud Consortium members are no strangers to BIN attacks and can speak at length on the harm caused to them and their customers.

One such member, a Payment Solutions Provider, experienced a fraud event early in the year and lived to tell the story. Not just one attack; they shared that they experienced over 150 attacks across all their BINs in under two months. The impact of these attacks reaches far beyond the immediate attack.

- **Processing and Interchange Fees:** These attacks translated to almost a million transaction attempts, and although many of those testing attempts were declines and ultimately unsuccessful, each of those attempts can mean numerous processing fees for a provider.
- **Business Disruption:** Almost 90% of these fraudulent transactions had chargeback rights, but the inconvenience, and cost of chargebacks, also ran up the provider's expenses.
- **Cardholder Disruption:** Not only does the business have to pay the network and the processor, but now the obviously compromised cards need to be replaced in hopes of halting the fraud – *typically at no charge to the cardholder*. Cardholder disruptions also opened the potential of damage the company's reputation.

Card testing for BIN attack fraud is often done through merchants which may have insufficient controls in place to prevent successful validation of a card number by a perpetrator – like online merchants without CAPTCHA, or address and CVV verification set up through their processor. Don't be mistaken however, smaller online shopping vendors without major controls in place, are not the only vulnerable companies.

For example, through the end of 2021 and continuing into 2022, FFC members, along with much of the industry, observed a significant BIN attack with companies as large as Google or Amazon. Bad actors compromised shopping and gaming apps which store card data, and systemically began processing in-app purchases using stolen and successfully tested cards. Although Google has controls in place, like velocity limits, the transactions circumvent these due to low dollar amounts, and the often-frequent nature of in-app spending for games.

The BIN attack using online gaming apps impacted around 50,000 of one FFC member's accounts alone – many large providers in the industry suffered losses in the millions overall – losses which could in some cases, be considered on top of the processing and transactional expenses caused by a BIN attack.

Limitations and Pain points

In discussions with our members, the FFC began to see commonalities in pain points amongst industry professionals.

Number one being that accountability and responsibility for the impact of a BIN attack is, some might say, disparately on the issuers, program managers, and payment processors. Other hurdles and pain points have included:

- **Reporting Thresholds:** Some partners within the industry may not even report BIN attack fraud, as the amount is often under their write-off threshold. Without the fraud from an attack being reported, volumes of attacks are mis-communicated or not communicated at all to the networks for potential downstream improvements.

> ***Some FFC members have even run into situations where the network has a potential threshold and began to advise that the merchant should be contacted directly instead. Some of these same merchants are simply un-equipped to combat the fraud.***

- **BIN Processing:** In an EMV chip world, we must consider our Prepaid partners and others, whose products are often on BINs which they have classified upon set up as Magnetic Stripe only. Even so, some have observed chip indicated transactions erroneously being approved through the network.
- **Expiration Dates:** Some Prepaid cards, such as open-loop gift cards, can be limited by card expiration rules. With that, a batch of cards from a BIN set that are created at the same time could all have the same expiration date making it even easier for perpetrators to capture that card data.

It's not all bad news; as a general trend FFC members have observed a decrease in BIN attacks. As we move to EMV chips the fraud activity is moving online to website authentication and Card not Present authorizations. Which in general gives us a more focused front to combat the fraud.

- **Help is Coming:** Networks are taking BIN and brute force attacks seriously. In some cases, they have dedicated groups who are creating prevention and detection methods to combat the fraud at card swipe and to be more accommodating when it comes to chargebacks. Future hope is that the industry may be able to shift some liability to merchants or acquirers without proper controls. Suggestions we gathered from networks included:
  - Tools like 3D Secure are available to help provide an extra set of parameters and controls
  - Pay attention to authorization response codes that might show up in spikes, like Expired Card or CV2 failure.
- **Employ CAPTCHA:** Where possible adding CAPTCHA can stop some of the automated bots and scripts from carrying out an attack entirely.
- **Don't be Predictable:** Avoid batch issuance of card numbers in sequential order. Where possible, and within regulations, change up expiration dates for cards in a BIN set.
- **Mix and Match Fraud Rules:** Normal fraud prevention methods like velocity limits have proven ineffective when deployed alone in stopping an attack. It is necessary to combine methodologies such as monitoring velocity and Merchant Category Codes, I.P. Addresses, and even monitoring declines.
- **Zoom out:** Many of our fraud controls are focused on looking at activity at the card level. With BIN attacks it may be more effective for us to take a step back and look for BIN Spikes to more quickly notice the beginnings of an attack. Adding alerts for chip transactions on a magnetic stripe cards only BIN could help catch unusual activity.

Solutions

A Case for Collaboration

A general question that we've been left with is...whose responsibility is it to prevent and detect a brute force attack like a BIN attack?

Who is in the best place to "catch" an attack when it starts, as well, who is it that suffers the most impact by an attack?

The best answer so far is that as an industry we **must** work together. No one entity along the transaction rails from merchant to network, to issuer, or acquirer can completely prevent or immediately detect an attack before it is "too late" all alone.

The FFC is one way to collaborate; join us in creating a working group of impacted companies to share best practices, gather data, and partner with the networks and acquirers in order to better combat this fraud.

FFC members get access to more detailed information as well as the ability to consult with subject matter experts with a broad range of experience.

Find out more by contacting us today!

online
fraudconsortium.org

email
info@fraudconsortium.org