AuditLink

SettleMINT EFT

MITIGATING BRUTE FORCE BIN ATTACKS

CU*ANSWERS

MAY 29, 2020

JIM VILKER & HEATHER FRENCH

OVERVIEW

On Presidents Day 2020 and the weeks following, several CU*Answers clients experienced brute force attacks on their ATM and debit card BINs. The losses suffered in some cases were in the six digits, which prompted the SettleMINT and AuditLink teams to dig in, understand how they happened, and what steps credit unions should consider to mitigate these losses.

This document will serve as a compilation of our findings and recommendations for ongoing monitoring.

JIM VILKER, NCCO, CAMS

Vice President of Professional Services, AuditLink

HEATHER FRENCH

Vice President of Managed Services, SettleMINT

WHAT IS A BRUTE FORCE ATTACK?

A brute-force attack is when a fraudster uses an auto-dialer to try to get the card numbers issued within your BIN. You will see attempted authorizations on card numbers not yet issued. These attempts will typically be on one merchant as they test cards to try to get authorizations. With a card number, fraudsters can perform unlimited guesses to find the card expiration date and other security layers to make the card usable. This impacts all card types including credit, debit, EMV or non-EMV, consumer or business accounts.

These attacks are well orchestrated by criminal rings. They not only include the compromise of the card account but also teams of people in the field waiting with activated cards to purchase goods via internet channels as well as physical stores.

HOW IS THIS DISCOVERED?

Ideally it would be uncovered by the switch, but unless the credit unions are monitoring for this specifically, it typically goes undiscovered until a member calls stating they have fraudulent transactions on their card.

In our research, we learned there could be signs of bad actors testing your BINs with card numbers prior to or as the attack is occurring. In some cases, the switch has fraud logic to detect this and requires a savvy employee to be reviewing the data who understands what to look for.

RECOMMENDATIONS FOR MITIGATING RISK AT YOUR SWITCH PROVIDER LEVEL

The following are recommendations that you should consider to lower the likelihood of almost any type for plastic fraud, including account take over due to phishing attacks, brute force BIN attacks, and criminals purchasing active cards on the dark web.

FOREIGN COUNTRIES

Do you have limitations on foreign countries and does your vendor offer travel letters for individual members who contact you regarding traveling to these countries? In one attack, almost all transactions originated out of Brazil and came through an unknown network.

Wondering what countries to block? That would be a great question for the fraud management departments at your vendor. FinCEN issued a March 26, 2020 advisory on this topic as well: https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets/advisories.

WHAT STRATEGIES OR SCHEMAS ALREADY EXIST AT THE SWITCH TO UNCOVER THESE?

Ask your vendor if they have strategies built in to uncover these types of attacks. This would include queries of the declined data that would lead one to believe your BIN is being tested or multiple transactions coming through the same merchant at high velocity.

These strategies use multiple variables including the fraud score, velocity, merchant type, geography, and many others. Push very hard on this question as our experience has been, they do not like to willingly give this information up. Also, ask what training they can provide for you to query the data to uncover fraudulent activity. This should be a skill set understood by credit union staff. Keep in mind, strategies like these do help stop these attacks, but you need to understand what your switch provides for free and what you need to pay for.

ANNUAL REVIEWS

Review your configurations every year including:

- Limits (where they exist and when they kick in);
- Any new fraud related tools that they have implemented or ones you can purchase;
- Alerts that would immediately tell you an attack is under way or fraud is evident;
- And any recommendations to lock the process down to mitigate risk.

If possible, have a fraud specialist from your vendor attend to help you understand what risks can be mitigated and what risks are emerging.

ALERT PROCESSING

Inquire as to whether alerts exist to notify you of excessive declines. Specifically, an uptick in transactions from the same merchant on cards that have not yet been produced. Are alerts configurable and do the vendor and credit union have escalation procedures to stop the fraud from growing at a fast pace?

STAND-IN PROCESSING

Ask your vendor about all stand-in possibilities outside of the communication to the core. What downstream networks are they connected to and what is the frequency that they go into stand-in?

In one case, all the transactions came through as force post and the vendor said they must have been approved while in stand-in, yet the stand-in process was not due to a

communication fault with CU*Answers. Does the vendor have additional fraud related systems that kick in while in stand-in?

TIMING OF EVENTS

Attacks frequently happen over holidays. Do you have staff checking the data or alerts and do you know what availability your vendor will have during these times? You want to make sure your vendor is willing to partner with you to alert you of potential fraud situations and help guide you to quick resolutions if discovered.

UNDERSTAND TRANSACTION FLOW

Understanding the transaction flow is important when trying to determine why you see approval/declines in one area. When a transaction is processed it goes through this process:

- → Member swipes at merchant
- → Merchant sends transactions through their preferred networks
- → Networks passes transaction to your vendor
- → Vendor passes transaction to your core

In the best-case scenario, all “stops” would be communicating with each other: merchant to the network, network to the vendor, vendor to the core. It is important to know that any of these “stops” could complete a stand in approval/denial. You should work with your vendor to understand what that means and what limits are in place.

It is also important to work with your vendor on understanding verification processes done at each of these steps. Is there verification at the merchant or the networks? What limits do they use if they cannot communicate with the vendor? What verifications are being done at your vendor? Are they validating the card number, that the PIN is correct, and the CVV code matches? What are the fraud verification processes you have in place? E.g. limits, transaction counts, name matching, etc.

Depending on how your vendor and core work together these items could be done on either side, so make sure when you are validating what is being done you are talking with both your vendor and your core.

UNDERSTANDING FRAUD MANAGEMENT

Learn what type of fraud service (e.g.: SecureLock) your vendor offers and how it can help protect your credit union. Please note, these services could incur additional charges.

It is also important to understand the software your vendor offers. Researching or monitoring transactions could allow your team to find an uptick in denials for cards not valid, invalid expiration dates, or possibly invalid CVV codes, which might alert you sooner to fraudulent activity underway.

By inquiring on these items, working with all your vendors, and learning about what you can take into your own hands, your credit union will be better positioned to prevent or mitigate fraudulent actions, including but not limited to brute force BIN attacks. The key items to take away:

Review existing configurations with your vendor

Review available loss mitigation controls with your vendor

Trend your metrics

AuditLink

SettleMINT EFT

CU*ANSWERS
6000 28th St SE
Grand Rapids, MI 49506
www.cuanswers.com