

Plastic Card Security Best Practices

working together to
prevent fraud and losses





Plastic Card Security Best Practices

Security Measure

Fraud Management Solutions

As a service to our Credit Union Bond policyholders, we have developed this checklist of best practices to evaluate your card program for fraud prevention and loss control. We recommend that you work with your card processor to properly set up your program and revisit your existing settings and control files on an ongoing basis.

Overview/Definition

In the world of plastic card fraud, the term “Neural Network” is used to describe a statistical model that evaluates plastic card account and/or transaction data.

Typically, the Neural Network Model generates a score for each account/transaction. The score separates those accounts/transactions that are likely to be fraudulent from those that are not. Accounts/transactions that receive higher scores are more likely to be fraudulent.

A robust Neural Network Model helps a fraud investigator focus on those accounts/transactions that are MOST LIKELY to be fraudulent.

A Neural Network Model is one component of a more complex Fraud Detection System. There are many other tools that are used to deliver and augment the score created by the Neural Network Model. These include:

- **Rule Systems** allow issuers and processors to focus more specifically on fraudulent accounts/transactions. Rule Systems typically incorporate a Neural Network Model score and allow the issuer to apply their own detailed knowledge to improve the process. For example:

If an issuer that typically reviews cases with a Neural Network score of 800 suddenly experiences an outbreak of fraud at electronic stores in Madison, WI, a Rule System would allow them to create a rule that says:

- IF the MERCHANT is ELECTRONICS
- AND the zip code is between 53701 and 53799
- AND the Neural Network Score is greater than 600
- CREATE A CASE TO REVIEW

In this case, the rule allows the issuer to focus on a specific fraud situation that would have been missed using the Neural Network score of 800. The important distinction is that “rules” can be modified by the user, while the Neural Network Model cannot.

- **Case Management Systems** refer to the PC workstation that a fraud analyst uses to review/work each case and determine the action that needs to be taken. A Case Management System usually allows the analyst to see recent transactions on the account, and provides the analyst with contact information so an attempt can be made to reach the cardholder. The Case Management System gives the fraud analyst enough information to make a decision in the event that a cardholder cannot be reached.

- **Authorization Systems** decide whether or not to approve or decline a transaction. The most basic Authorization Systems will make this decision using elements such as:
 - Available Credit Limit/Account Balance
 - Current Status (is the account overdue?)
 - Open/Closed Indicator
 - Expiration Date Check
 - CVV Validation

This example is greatly simplified. Most Authorization Systems are much more complicated and offer the issuer a great deal of flexibility in determining which authorizations should be approved or declined based on the issuer’s individual desire to balance risk and cardholder convenience.

While the Neural Network Model can help predict which accounts/transactions are most likely to be fraudulent, it requires follow-up action to verify the activity or to decide whether or not an account should be blocked. The other components of the Fraud Detection System and Authorization System help credit unions and processors take action to identify and stop fraudulent activity as quickly as possible.

Fraud Management Solutions

—continued

Fraud Management Solutions

- Verify that each of your card portfolios (credit card, debit card and ATM cards) is protected by a Fraud Detection System. This includes the use of a predictive Neural Network Model.
- There are many fraud detection tools available today. Educate yourself on the tools that are available to you, and what capabilities you have to modify Rules and Authorization Systems to control fraud losses.
- We recommend evaluating the Visa® Advanced Authorization score as a tool to help reduce fraud resulting from merchant data compromises.
- Make an informed decision on which tools to use based on performance. Choosing fraud tools based on cost alone often results in high fraud losses in the long-run.

Debit Card and ATM Card Issuers

- If you issue “ATM ONLY” cards, be sure that you know WHERE and HOW those authorizations are processed, and what fraud tools are available to protect them.
- If you issue Visa Check Card or Master Money debit cards, understand that although there is only ONE card, PIN and signature authorizations can be handled on completely different Authorization Systems. Again, it’s important to know WHERE and HOW those authorizations are processed, and what fraud tools are available on each Authorization System.
- Know where both types of transactions are processed. Understand the data used to make the authorization decision and the tools available to improve those decisions.

Real Time Capability

- Your Fraud Detection System should be capable of identifying high risk accounts and automatically “block” (suspend charging privileges) when necessary.
- The Neural Network Model score should be delivered in “real time.” This means that the Authorization System should receive the Neural Network Model score in time to make the decision to approve or decline a transaction.
- “Rules” that can be written to augment the Neural Network score should also be capable of running in real time.

Case Management

- Provide fraud analysts to work cases 24 hours/day, 7 days/week, 365 days/year. It is imperative that a fraud analyst be able to review a potential fraud case and decide whether or not to block an account at any time when a case is created—whether or not the cardholder can be reached. Waiting for cardholder contact will lead to increased fraud losses.
- Credit unions should NOT serve as an intermediary between a fraud analyst and the cardholder. The delay increases fraud losses. This delay can be extremely costly if fraud alerts are received by a credit union after hours, or on weekends and left unattended for long periods of time.

Member Education

- Educate your members about fraud protection. Many issuers position their fraud detection efforts as a service that they extend to “protect” their cardholders.
- Consider the marketing campaigns that you have seen in major media outlets that revolve around fraud detection. The message is that protecting the customer is a service, not an intrusion.
- If you have access to the fraud Case Management System, consider asking cardholders to contact you when they intend to travel. Comments placed in the system can help fraud analysts quickly and accurately handle cases if activity from a traveling cardholder raises suspicion.

CVV/CVC and Card Based PIN-Offset

ALL Visa and MasterCard® branded plastic cards include a “CVV” or “CVC” encoded on the cards magnetic stripe. This is a critical security feature since it is invisible to the cardholder and cannot be accidentally disclosed.

As a requirement of Visa and MasterCard, CVV/CVC is verified on every CREDIT CARD purchase and every DEBIT CARD purchase that is completed USING A SIGNATURE.

CVV/CVC can also be verified on ALL ATM and PIN based transactions that use a Visa or MasterCard branded plastic.

If CVV/CVC is NOT being used on ATM or debit PIN transactions, it becomes easier for a criminal to obtain enough data to create a working counterfeit plastic card that can be used to withdraw funds directly from an ATM Machine.

For “ATM only” portfolios that are not co-branded with Visa or MasterCard, CVV/CVC is not often available. For these portfolios, many issuers substitute a “Card Based PIN-Offset” for CVV/CVC.

The Card Based PIN-Offset is a numerical value that is coded on the magnetic stripe of the card. When an ATM transaction takes place, an algorithm on the Authorization System uses the entered-PIN and elements of the card number to calculate the “expected” PIN-Offset number.

The expected PIN-Offset number is then compared to the Card Based PIN-Offset that appears on the transaction. If they match, the transaction is approved.

Just like CVV/CVC, a Card Based PIN-Offset is an important piece of data that cannot be disclosed accidentally by the cardholder.

- Ensure that CVV/CVC is encoded and validated on all magnetic stripe authorizations, including:*
 - ALL Signature Credit Transactions
 - ALL Signature Debit Transactions
 - ALL PIN-Based Debit Transactions
- Verify that when a transaction is received WITHOUT a CVV/CVC, the transaction is DECLINED.*
- Verify that when a transaction is received with a CVV/CVC that DOES NOT MATCH the expected CVV/CVC, the transaction is DECLINED.*
- Verify that if a transaction is DECLINED because it included an incorrect CVV/CVC or because there was no CVV/CVC, that the card is blocked and that a new card is issued to the cardholder.
- Block the card immediately after a maximum of TWO transactions with no CVV/CVC or a mismatched CVV/CVC.
 - This is important because criminals will make numerous attempts to guess the correct CVV/CVC in order to create a counterfeit card.

For “ATM only” cards:

- Consider using a Card Based PIN-Offset

*Note: Plastic Card/PIN Endorsement Requirement

Security Measure	Overview/Definition	Best Practices
<p>Name Matching for Track 1 Magnetic Stripe Data</p>	<p>The cardholder’s name is encoded on the card’s magnetic stripe.</p> <p>Depending on the point-of-sale terminal that is being used, the cardholder’s name can be:</p> <ol style="list-style-type: none"> 1. Printed on the receipt. 2. Transmitted as part of the authorization request. <p>Often, criminals will carry fake identification and will encode a matching name on the magnetic stripe. This enables the criminal to produce ID if requested by the merchant, and to re-use the same fake ID for multiple counterfeit cards.</p> <p>When the criminal changes the name on the magnetic stripe to do this, the new name on the magnetic stripe will NO LONGER MATCH the name on the Authorization System.</p> <p>Making sure that the name transmitted on the magnetic stripe matches the name on the Authorization System provides issuers with a good opportunity to reduce losses due to counterfeit fraud.</p>	<ul style="list-style-type: none"> • Verify that the name transmitted from the magnetic stripe in the authorization is compared to the cardholder name used by the Authorization System. • Ensure that this comparison is done for ALL card programs. • Confirm that when the names do not match, the authorization is DECLINED. • Ensure that you standardize the way in which names are formatted on the cards, Authorization System, and other systems involved in the process. This will eliminate any mismatches due to differences in punctuation, abbreviations, etc.
<p>Exact Cardholder Expiration Date</p>	<p>All credit and debit cards have an “expiration date” encoded onto the magnetic stripe in the month/year format.</p> <p>When a transaction is received, the Authorization System typically checks to make sure that the date on the card MATCHES the date on the Authorization System.</p> <p>It is important when verifying the expiration date that the Authorization System is looking at the EXACT month/year. In the past, some issuers have permitted a “range” of valid dates. This practice is ineffective.</p>	<ul style="list-style-type: none"> • Understand where the comparison of expiration dates takes place in the authorization process. • Confirm that the exact expiration date is validated on all “card present” and “card not present” Visa/MasterCard signature authorizations (“card present” is a contract requirement).* • Confirm exact expiration date is validated on all Visa/MasterCard PIN based authorizations.* • Confirm that the exact expiration date is validated on all ATM network cards (non Visa or MasterCard). • Verify that when a mismatch occurs, the transaction is DECLINED. • Block card if multiple transactions are received with a mismatched expiration date AND the magnetic stripe was used in the transaction. <p>*Note: Plastic Card/PIN Endorsement Requirement</p>



Daily Limits

As soon as a criminal obtains a functioning plastic card, they will spend money as quickly as possible until they are stopped.

Issuers are able to prescribe “daily dollar limits” that restrict the total amount of money that can be spent using a card during the course of a single day.

Daily limits are an important safeguard that limit a credit union’s exposure in the event that other controls and attempts to verify transactions are unsuccessful.

It is important to note that there are often two SEPARATE daily limits; one that governs ATM-PIN based transactions and one that governs signature based transactions.

A second type of limit applies to the number of transactions that can be attempted in a single day. This is referred to as “transaction velocity.” Often, criminals will attempt numerous authorizations in order to “test” accounts, and to find missing pieces of data, such as a PIN, CVV/CVC or expiration date.

- Verify that all card programs have a daily dollar limit. If your credit union elects to offer a daily dollar limit greater than the amounts listed below, you may share in the risk of additional fraud exposure beyond the recommendations.
- For Visa/MasterCard credit cards, it is recommended that credit unions do NOT use the credit line as the daily limit. Consider limiting the maximum daily limit for cash advances to:
 - \$10,000 for Visa/MasterCard credit purchases.
 - \$1500 for Merchant Category Code 6010 (Teller Window)
 - \$510 for Merchant Category Code 6011 (ATM)
- For Visa/MasterCard debit cards, credit unions should limit activity to:
 - \$1500 for signature based transactions
 - \$510 for PIN based transactions
- Transaction velocity limits should be applied to all card programs.
- It is important that daily dollar and transaction velocity limits function independently, so that exceeding either can cause an account to be reviewed or blocked.

Card Activation and Card Mailing

“Card activation” refers to the practice of shipping cards that cannot be used until the recipient contacts the issuer to confirm that they have received the card. Card activation is a simple but effective way to prevent use of a card by a criminal who steals plastic cards from the mail and begins charging without the cardholder being aware that a card is in circulation.

Usually, the cardholder is asked to provide some form of information to authenticate recipient.

This can be done automatically through systems that recognize the phone number from which the recipient is calling and then confirm that the number matches the account records.

Card activation can also be done by a live service representative who requests one or more pieces of information that only the correct recipient would be able to access.

There are several instances in the account lifecycle where card activation applies:

- **Newly Issued Cards**—a new account is opened and a plastic card is delivered to the customer.
- **Renewal Cards**—the expiration date arrives and a new plastic is delivered to the cardholder.
- **Replacement Cards**—a card is lost, stolen, damaged or in some other way not usable and must be replaced.
- **Additional Cards**—a cardholder wishes to add a joint account holder, authorized user, etc.

- Verify that card activation is used on all credit and debit card programs*
- Verify that card activation is used on the following:
 - Newly issued cards
 - Renewal cards
 - Replacement cards
 - Additional cards
- Ensure that as soon as a new card is activated, the old card is closed and blocked from future use.
- Use an effective activation method. Consider the following:
 - PIN activation that requires a cardholder’s first transaction to be PIN driven. This works well for debit and ATM cards.
 - Calling from a home telephone number so that the phone number from the incoming call can be matched against your customer records. Consider requesting one additional piece of information along with this approach.
 - For renewal cards, consider using the CVV2/CVC2 value from the expiring card to activate the new card.
 - If the credit union is performing the activation, consider using data from your member system that would be known only to the cardholder.
- Card mailings should be disguised as much as possible.
- Always mail cards and PINs separately.
- Ensure that cards are mailed “inactive” with \$0 allowable authorization until card activation is complete.

*Note: Plastic Card/PIN Endorsement Requirement

Security Measure	Overview/Definition	Best Practices
<p>Address Verification Service (AVS)</p>	<p>Address Verification Services can be requested by a merchant at the time of authorization. These requests occur commonly when the card is not present for the transaction (such as mail order, telephone order or Internet purchases).</p> <p>If the merchant requests an “address verification” at the time of purchase, the issuer must respond or risk forfeiting chargeback rights if the transaction is later disputed.</p>	<ul style="list-style-type: none"> • Confirm that you can respond to address verification requests for all Visa/MasterCard authorizations when the merchant transmits an AVS request.* • Confirm that you are providing verification based only on exact matches. • Maintain current cardholder address information in order to reduce fraud exposure and avoid member service issues related to AVS responses. <p>*Note: Plastic Card/PIN Endorsement Requirement</p>
<p>CVV2/CVC2</p>	<p>CVV2/CVC2 is the three digit code that appears in the upper right hand corner of the signature panel on the reverse side of ALL Visa and MasterCard credit cards and debit cards.</p> <p>While the CVV/CVC codes mentioned previously are NOT VISIBLE to the cardholder, the CVV2/CVC2 are CLEARLY VISIBLE.</p> <p>The purpose of the CVV2/CVC2 is to enable the issuer to better authenticate the user of the card during a telephone or Internet transaction.</p> <p>When you are using the card for an Internet or telephone transaction, a MERCHANT will generally ask you for this number. When the merchant creates a “card not present” (CNP) transaction, the CVV2/CVC2 is included.</p> <p>When the transaction arrives at the issuer or processor, they are able to verify that the number provided matches the one they expect to receive. This provides assurance that the actual card is being used for the purchase.</p> <p>CVV2/CVC2 is usually validated in conjunction with some other piece of personal data.</p>	<ul style="list-style-type: none"> • Verify CVV2/CVC2 for all transactions when CVV2/CVC2 is transmitted by the merchant* <ul style="list-style-type: none"> —This includes all transactions where the card is not present (Internet, mail order, telephone order), or when the magnetic stripe is not being processed (i.e., keyed transactions). • Verify that a mismatch between the provided and expected CVV2/CVC2 results in authorization being DECLINED.* <p>*Note: Plastic Card/PIN Endorsement Requirement</p>



Security Measure	Overview/Definition	Best Practices
<p>Online (Internet) Card Security: Verified by Visa (VBV) and MasterCard SecureCode™ (MCSC)</p>	<p>Both Visa and MasterCard have established programs designed to reduce fraud losses on Internet transactions.</p> <p>Both “Verified by Visa” and “MasterCard SecureCode™” allow a cardholder to create their own unique password that can be verified by the issuer when the card is used for Internet purchases.</p>	<ul style="list-style-type: none"> • Confirm that your credit union is participating in Verified by Visa (VBV) and/or MasterCard SecureCode (MCSC) for all online purchases when the online merchant requests VBV/MCSC in the authentication process. (MasterCard has mandated SecureCode™ for all card issuers).** • Verify that your cardholders are enrolled.** • Confirm that your CAVV (Visa) and AAV (MasterCard) are set to DECLINE for mismatches.** <p>**Note: The Plastic Card/PIN Endorsement covers fully authenticated authorizations for online (Internet) transactions.</p>
<p>Issuers’ Clearinghouse Service (ICS)</p>	<p>Issuers’ Clearinghouse Service (ICS) helps verify an applicant’s address, phone number and Social Security Number.</p> <p>ICS is a useful tool in identifying data that has been used fraudulently in the past as well as data that is being used excessively for applications.</p> <p>ICS is mandatory for all credit card and U.S. card issuers.</p>	<ul style="list-style-type: none"> • Confirm that all of your applications (approved and denied) are provided to ICS. • Submit all verified fraudulent applications to ICS immediately. • Consider using ICS to verify information for all new membership, new card applications, requests for address changes and other changes to account data.
<p>New Account/ Existing Account Address Validation</p>	<p>Validation of address information helps control fraud losses due to identity theft and account takeover.</p>	<ul style="list-style-type: none"> • Confirm the use of an identity theft solution to verify member addresses and changes to addresses. • Consider centralizing address change data to detect any “common” addresses/locations that are being used. • Verify address changes by mailing confirmations to BOTH the NEW and OLD addresses. • Apply a waiting period prior to issuing funds, plastic cards, or PINs. • Track suspicious applications or account changes for at least 30 days. • Ensure FACT ACT compliance.



Security Measure	Overview/Definition	Best Practices
<p>Cardholder Dispute and Recovery</p>	<p>The Cardholder Dispute and Recovery Process provides important protection for cardholders and issuers.</p> <p>The process shifts the responsibility for some charges/purchases to the merchant or their acquiring institution when specific processes (mandated by the card associations) have not been followed, or when processing rules have been broken (i.e., merchant data compromises).</p>	<ul style="list-style-type: none"> • Pursue exhaustive recovery attempts through chargeback and compliance/pre-compliance.* • Confirm that you and your card processor provide awareness training for (1) chargeback rights and (2) pre-compliance/compliance rights (i.e., merchant data compromises). • Establish a timely process for reviewing cardholder claims, determining which claims merit a recovery attempt, and executing those attempts. <ul style="list-style-type: none"> —Consider assigning responsibility for this task to a specific individual. —If a third-party processor is filing compliance/pre-compliance claims on your credit union’s behalf, ensure that the processor is receiving your credit union’s Visa CAMS and MasterCard Alerts. • Track chargeback recovery amounts. You should be able to compare the amount of total fraud claims that were successfully challenged. • If a cardholder identifies fraudulent transactions on their account, be sure to block the card from further activity. <p>*Note: Plastic Card/PIN Endorsement Requirement</p>
<p>Other Security Measures</p>	<p>Here are a few other recommended strategies to reduce fraud and losses.</p>	<ul style="list-style-type: none"> • Limit your credit union’s BIN range to a reasonable number. • Allow members to select their own PINs when possible.



This information is for the sole use of our Credit Union Bond policyholders and is proprietary and confidential to CUNA Mutual Group. Any further reproduction, adaptation or distribution is prohibited.

The Credit Union Bond is underwritten by CUMIS Insurance Society, Inc., a member of the CUNA Mutual Group.



CUMIS Insurance Society, Inc.

P.O. Box 391
5910 Mineral Point Road
Madison, WI 53701-0391
1.800.637.2676
www.cunamutual.com