

EMV Card Fraud: Can Your Fraud Detection System Identify Suspect Chip Card Transactions?

While EMV (chip) cards offer increased security and significant reduction of fraud, chip-and-PIN technology cannot eliminate EMV card fraud entirely. As an EMV card issuer, you must test your fraud detection system to ensure that when suspicious chip card transactions occur, they are promptly identified.

While EMV (chip) cards offer increased security and significant reduction of fraud, chip-and-PIN technology cannot eliminate EMV card fraud entirely. As an EMV card issuer, you must test your fraud detection system to ensure that when suspicious chip card transactions occur, they are promptly identified. What methods can your fraud detection system use to identify some of the most common EMV card fraud scenarios? This article presents a sampling of these scenarios and illustrates how pre-production testing of your fraud detection system can reduce your risk of certain types of EMV card fraud.

Track the number of invalid Authorization Request Cryptograms (ARQCs)

Why:

Just as a valid Authorization Request Cryptogram (ARQC) indicates valid data; multiple invalid ARQCs from a single EMV card likely indicate the transaction data has been altered.

Detection Strategy:

The fraud detection system should track the number of bad ARQCs that a chip card generates using a velocity limit. A fraud detection system's velocity limit, when exceeded, triggers a specific action by the card or terminal. The fraud detection system can trigger an application block to prevent fraudulent use until the suspicious circumstances are investigated with the cardholder or merchant. (Blocking an EMV card is an alternative but, because a blocked chip card is rendered useless and cannot be reactivated, card blocking is typically reserved for lost or stolen EMV cards.)

Test Plan:

Use a scripted test tool with a soft card database that enables you to alter transaction data for a specific test chip card and generate a sufficient number of transactions to exceed the velocity limit for your fraud detection system. Test to ensure that for any subsequent transaction by that test chip card that the proper action is taken.

Track the number of fall-back transactions from the EMV card

Why:

A fall-back transaction indicates a device encountered a problem performing the desired transaction with the chip, so the device “falls back” to processing the transaction as a magnetic strip transaction. (The device still connects to the host to send the magnetic strip transaction request online.) A card that always reverts to a fall-back transaction can be an indication of damage to the chip coupled with re-writing the magnetic stripe and altering the service code.

Detection Strategy:

When the fraud detection system identifies that transactions from an EMV card at a chip-capable terminal are repeatedly being forced into fall-back magnetic strip transactions, those transactions should be flagged as fraud suspects. Issuers should track these occurrences and decline subsequent transactions from that chip card with an appropriate action code.

Test Plan:

Use a test tool to generate an excessive number of fall-back transactions for a test chip card. (There are two ways to change the service code value: generate a number of transactions with various service codes using a scripted test tool that enables automatically overriding the existing service code with any desired value at test run time, or using a soft card database that enables you to quickly make changes to the values in the EMV card record.) Test to ensure that any subsequent transaction by that test card triggers the proper action.

Track the number of times the EMV card sends a “PIN tries exceeded” notification

Why:	The card tracks the number of invalid PIN tries. Even legitimate cardholders may forget or erroneously enter their PIN, but multiple instances of invalid PIN tries may indicate fraudulent chip card use.
Detection Strategy:	The fraud detection system should track the number of times an EMV card notifies the card issuer that the PIN tries have been exceeded. When PIN tries are exceeded more frequently than the established limit, the fraud detection system can notify the issuer to take the appropriate corrective action (perhaps notifying the customer to contact the issuing institution).
Test Plan:	Use a test tool to generate offline transactions that use an invalid PIN for the test chip card. Test to ensure that the "PIN Tries Exceeded" notices from the chip card are triggered and that the proper action (as specified by your organization) is taken.

Monitor multiple EMV card transactions from diverse geographies

Why:	Obviously, no one can be in more than one location at a time. Similarly, although long-distance travel is more common now than for previous generations, EMV cardholders are unlikely to use their chip cards in several diverse geographical locations within a limited time.
Detection Strategy:	Fraud detection systems can monitor the regions from which a chip card's transactions originate. Actions may include forcing an EMV card on-line so the issuer can block the chip card.
Test Plan:	Use a test tool to simulate transactions from a single test chip card occurring in multiple regions within a narrow time frame. Also simulate transactions in multiple regions occurring over multiple days from a single test chip card. Test to ensure the fraud detection system flags the EMV card's transactions as suspect.

Identify inconsistent tag values in EMV card transactions

Why:	Like the invalid ARQCs mentioned previously, tag values that provide conflicting information about a transaction may be chip card fraud indicators.
Detection Strategy:	Fraud detection systems can monitor tag values for CVR (card verification results). For example, the Application Usage tag (9F07) contains information (a sub-element) that indicates whether or not the chip card is allowed for use in international cash-back transactions. The issuer host can use the value in this tag with the processing code and other fields in the EMV message to decide if this transaction is actually allowed for the chip card.
Test Plan:	Use a test tool to simulate transactions that include inconsistent tag data. Test to ensure the fraud detection system flags the EMV transactions as suspect.

Need Help Testing Your Fraud Detection System for EMV card fraud?

Paragon Application Systems has testing solutions to help you create diverse testing scenarios for chip card fraud, as well as other types of EMV testing. You can efficiently set up multiple testing scenarios using soft cards and easily configured terminals. The same test cases are available for subsequent importing into stress and load testing tools. Visit Paragon Application Systems at www.paragonedge.com to learn more.

About Paragon Application Systems

Paragon Application Systems is a leading global provider of ePayment simulation, configuration and testing software tools to the financial industry. More than 400 financial institutions in over 80 countries use Paragon tools to improve quality and reduce time-to-market. Paragon's broad customer base includes major interchanges, processors, leading software providers, banks and credit unions. Visit Paragon Application Systems at www.paragonedge.com.

About the Author

Harold Pruitt, a Solutions Architect at Paragon Application Systems, provides EMV training and hands-on assistance to customers world-wide who are implementing Paragon's EMV testing solution. Harold has extensive experience with EMV and a thorough understanding of EMV cryptogram generation, as well as standard message data encryption using both single and triple DES. He has over 20 years of financial industry experience at companies including Veriphone and S2. Harold is a graduate of the University of Houston with a degree in Philosophy.