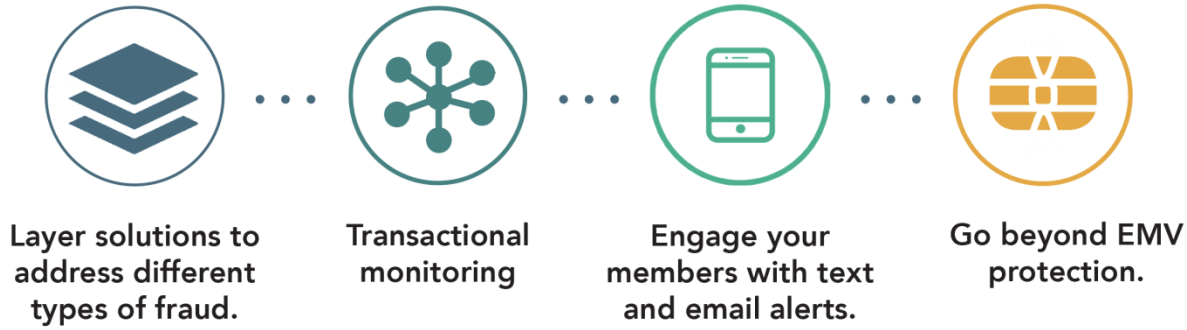
Best Practices for Preventing and Managing Card Fraud

Fraudsters and cyber criminals look for weak points in systems to gain access to information and data. It is a lucrative business. ATM skimming is seeing a resurgence and card-not-present fraud has increased since EMV has been implemented. Fraud schemes are constantly shifting.

How do Credit Unions protect themselves?



- Layer solutions to address different types of fraud. Gone are the days of setting up fraud solutions to cover the basics and thinking breaches happen to someone else. If you have something of value, criminals will try to take it. Are you prepared?
- Transactional monitoring for payment cards is basic to any fraud system. Neural networks monitor risky transactions, score, and alert members to possible fraud. Fraud predictor models enhance the basic setup by identifying merchants and ATMs that are more or less likely to have fraud. Machine learning technology is another enhancement. Adaptive models self-learn to improve predictions of future fraud behavior. These tools together dramatically improve the overall accuracy of the neural network.
- Engage your members in fighting fraud.
    - Email and text messaging notify members of suspicious transactions. Members can respond to the alert and validate transactions. This helps stop fraud sooner and get the card blocked if necessary.
    - A mobile app can help members can take control. They can turn a card on/off, set up alerts, and set limits and types of transactions.
- Go beyond EMV protection. EMV and Fallback limits have decreased fraud in card-present environments, but fraud is moving to card-not-present transactions. To combat CNP fraud, the 3D Secure 1.0 solution (Verified by Visa and MasterCard Secure Code) has moved away from static passwords to a risk-based authentication method. Updates in 2019 will increase available validation data for the authentication process.

New tools exist to help identify big and small compromises and calculate the likelihood of a future breach. Other new tools search the dark web and identify BINs for sale or those already sold.

Other add-on fraud services include customized fraud-strategy programs that address fraud specific to each issuer's portfolio. Browser-based tools also help credit unions effectively and efficiently manage compromised credit and debit accounts for both Visa alerts and MasterCard fraud events.

Cybercriminals aren't content with the status quo. As the value of some forms of data falls, they look for different channels and improve their tactics. Don't leave your Credit Union vulnerable!

Have more questions about preventing fraud? Please contact SalesTeam@LSC.net for a consultation.