Point of View

The Defense Never Rests

Fraudsters exploit uncertainty. Be prepared, inform cardholders and use advanced risk mitigation tools and services to enable them to spend with confidence.

Consumer fraud losses can add up, even when transaction volumes are down. Here are some tips to protect your payments program.

Remind Cardholders of Current Fraud Trends

Cardholders should be aware of the following types of fraud:

- Charity scams – Solicitations from unfamiliar charities, calls from unknown or blocked phone numbers or emails from unrecognized accounts are suspect; encourage cardholders to withhold contributions until they've fully vetted the organization
- Account takeovers – Fraudsters who gain key details of an individual's account can make card purchases, withdraw funds or access other accounts; promote regular account monitoring of all account activity

Help Accountholders Help Themselves

The best line of defense against fraud is an engaged and proactive consumer. Encourage vigilance: if something sounds suspicious it probably is. Advise accountholders to review their accounts daily and report unauthorized activity immediately. Remind them to:

- Keep an eye on their money by monitoring account balances
- Safeguard personal information; don't disclose Social Security numbers, Personal Identification Numbers (PINs), passwords or other identifying information tied to accounts or cards
- Be cautious when using remote terminals or kiosks including pay-at-the-pump gas and standalone ATMs

Review Risk Rules

Adjust your neural network scoring model to account for changes in consumer spending. In particular, ensure you reduce false positives that result when a valid transaction is denied. Use data-driven technology to balance fraud versus friction. Your objective should be to optimize payment experiences by maximizing cardholder approvals while mitigating fraud.

Review Program Controls

Authorization controls are the building blocks of effective transaction processing. Set appropriate parameters to maximize risk mitigation.

Establish Appropriate Transaction Limits

Transaction limits identify the maximum dollar amounts allowed for specific transaction types, such as ATM and Point-of-Sale (POS), within a given time period. Review current limits for cash withdrawals and purchasing activity based on current economic circumstances and consumer spending profiles. Define appropriate amounts to safeguard your consumers against card abuse.

Review Consumer Spending Velocity

Velocity support defines the maximum number of times a card can be used for ATM, POS or cash-equivalent transactions within a specified time interval. Be mindful that card usage varies widely among consumers. Remain nimble and adjust velocity limits to account for individual usage patterns.

Review Current Products and Services

Additional tools can be used to mitigate fraud and enhance the consumer experience.

Personalized Card Controls and Alerts

Enable cardholders to define when, where and how their cards are used. Enable them to receive transaction alerts and manage their debit and credit card usage through your mobile banking app.

Fraud Warning Services

Early detection tools can notify you weeks before a network alert and pinpoint small and local compromises not typically investigated by the networks. These services allow for early and accurate identification of compromised cards.

Rule Exemption Services

Uncharacteristic consumer purchases may be denied with an alert delivered asking for transaction validation. With an automated exemption service, after an alert is closed as no fraud, an exemption can be automatically applied to risk applications and rules, allowing for future transactions to be completed without any inconvenience or additional intervention from you.

Texting

Automated voice and email notifications sent to consumers may be missed or ignored. Consider text messaging for convenience and speed. Real-time consumer responses can prevent payment disruption and minimize fraud exposure.

Tokenized Transactions

Encourage adoption of digital wallets that leverage tokenized transactions. Safer than traditional card-based transactions, these methods transmit data protected through encryption.

Keep Your Consumers Safe

As fraud evolves, evaluate and implement risk management strategies to help you strike the balance between mitigation and a frictionless consumer purchasing experience. Proactive approaches are the key to defending your financial institution and cardholders.

About the Author

Patrick Davie is vice president, product strategy for Card Services at Fiserv. Patrick and his team develop and deploy risk management services supporting debit and credit transaction processing.

Connect With Us

For more information about Card Services, call 800-872-7882, email get solutions@fiserv.com or visit fiserv.com.

Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimising. Our solutions help clients deliver financial services at the speed of life to enhance the way people live and work today. Visit fiserv.com to learn more.

Fiserv, Inc.
255 Fiserv Drive
Brookfield, WI 53045

800-872-7882
262-879-5322
getsolutions@fiserv.com
www.fiserv.com

578463 04/20