Card Risk Solutions

December 9, 2019

Risk Office Advisory 19800

Cardholders and Holiday Scams

☒ **311: Informational; No Action Required**
☐ 611: Need to Know; Action May Be Required
☐ 911: Urgent; Action May Be Required

Debit Card & ATM Programs
Credit Gateway Programs
Full-Service Credit Programs

Summary
This Advisory from our Risk Office discusses various fraud schemes your cardholders may encounter this holiday season, and how you can help them avoid falling victim.

Fraud schemes are hardly limited to the holidays, but they tend to spike during this high-spending and stressful time of the year. The Fiserv Risk Office would like to help you arm your cardholders with information on the fraud practices they may encounter and how to avoid becoming a victim.

Technology has created many more options for cardholders to access accounts and make purchases, fraud too has opened up more sophisticated avenues. But it is always good to remind your cardholders of the basics: to continue to be skeptical about calls, texts, and emails. Your staff should also keep in mind that fraudsters often impersonate cardholders to request a change in contact information or a travel exemption to lower your fraud defenses.

Here is a refresher of several important fraud methods your cardholders may see:

Brute Force schemes are attempts to crack a password or username, find a hidden web page, or find the key used to encrypt a message using a trial-and-error approach to guess correctly. This is an old attack method, but it's still effective and popular with hackers as they work, whether to crack a single card number or complete BIN.

Skimming is perpetrated by using electronic devices to surreptitiously scan and store credit and debit card numbers and PINs. ATMs and some unattended terminals, such as gas stations, are targets for this practice. This information can then be sold to fraudsters or used to commit theft directly. Fraudsters can use the numbers to make online purchases or to create fake cards for in-store transactions.

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

SMiShing (SMS phishing) is the act of attempting to acquire personal information such as passwords and details by masquerading as a trustworthy entity through SMS text messages on cell phones. SMiShing messages may come from telephone numbers that are in a strange or unexpected format with links directing to fake websites.

A typical SMiShing occurrence can begin with a cardholder receiving a text message inquiring about a suspicious transaction on an account. In reality, the fraudster is looking to obtain other information from cardholders such as debit/credit card numbers, CV2 codes, expiration dates, PINs and other web login credentials.

Please let your cardholders know that legitimate SMS text messages from Fiserv will NEVER include:

- Requests for cardholder's data, such as card numbers, PINs, CV2 Codes, or Expiration Dates
- Vague reference of a "merchant" transaction; details should be included
- Hyperlinks to unknown websites
- Phone numbers as hyperlinks

Criminals in possession of card details and other forms of personally identifiable information (PII) may be able to spoof your financial institution's phone number to fool cardholders into thinking text messages are from your fraud department.

Vishing is the telephone equivalent of phishing. It is described as the act of using the telephone to scam the user into surrendering private information that will be used for fraudulent purchases or identity theft.

Some holiday scams your cardholders may see:

Seasonal Travel Scams

- Beware of deals that are too good to be true
- Cardholders should always know who they are booking their travel through

Holiday Charity Scams

- A legitimate charity will welcome donations whenever the cardholder chooses to make it. Fraudsters will pressure them to make it immediately.
- Don't make any donation with a gift card or wire transfer.

Account Takeover

- All user information is targeted in data breaches, not just payment card information.

- As fraud controls get smarter, fraudsters are shifting their strategies and patterns to bypass controls.

We recommend you directly contact your cardholders with as many reminders as possible through email, text, mailers, and banners on your website. Here are some Fiserv solutions to aid in fraud mitigation and customer empowerment:

Automated Risk Exemption Service (ARES)

- Allows customers to continue using their card after a suspect transaction is confirmed to be Not Fraud.

Step Up Authentication

- Enhanced cardholder authentication during contact center calls.

Fraud Warning

- Proactive notification of card compromises in advance of network alerts.

SMS Texting

- EnFact alert notifications and responses via text.
- Allows EnFact cases to be confirmed and statused quickly.

CardValet

- Customers can turn their own card on or off, or set restrictions on transactions by type, location, or amount.
- Customers can set their own notifications for transactions by type, location, or amount.

If you have any fraud-related questions, or want more information on adding a risk solution, please reach out to your risk analyst or your Card Services client executive.