PSCU

PERSPECTIVES

A CISO's Tips for a Fraud-Free Holiday Season

December 2015

While the holiday season traditionally brings consumers words of warning about an increased risk of fraud, vigilance on the part of credit unions and consumers can go a long way towards a fraud-free holiday season.

Read on for a list of ways credit unions and consumers can protect themselves during the holiday shopping season, courtesy of PSCU.

Credit Unions: Prepare Your Members

1. Make fraud-prevention tools like EMV available to your members then teach members how to utilize them.

2. Educate members on best practices regarding use of their cards.

3. Have your Bank Identification Numbers (BINs) tokenized. Existing BINs can be tokenized, so there is no need to reissue cards in order to enable tokenization. Once this is complete, you'll be better positioned to offer digital wallets that leverage tokenization technology; wallet providers will be able to request tokens for your cards they have on file.

Gene Fredricksen
VP Enterprise ITS Security, PSCU

Gene Fredriksen is the CISO for PSCU. In this role he is responsible for the development of information protection and technology risk programs for the company. Gene has over twenty five years of Information Technology experience, with the last twenty focused specifically in the area of Information Security. In this capacity, he has been heavily involved with all areas of Audit and Security. He is a Distinguished Fellow for the Global Institute for Cyber Security and Research, headquartered at the Kennedy Space Center. The Institute is a partner with the Department of Homeland Security, other agencies, academia, private industry and organizations focusing on the advancement of Cyber Security. In 2007 and 2015 Gene was named one of the Top Three Security executives in the US. In October 2015 he was named the CISO of the Year by The Tampa Bay Technology Forum.

A CISO's Tips for a Fraud-Free Holiday Season

4. Enroll in digital wallets that use tokenization such as Apple Pay, Android Pay and Samsung Pay so your card art will be present when your cardholders use these applications.
5. Make tools like member alerts and fraud alerts readily available to your members.
6. Educate members on phishing and how to recognize it.
7. Compile a list of resources and tips to help members monitor their own accounts, along with steps to take if they suspect fraudulent activity.
8. Recognize that the EMV liability shift deadline for ATMs is still on the horizon, which may make them a target for fraudsters. Educate members about this altered ATM environment, and consider implementing tools that help reduce the impact of attempts to use stolen information to withdraw cash from your ATMs.

Checklist to Share with Consumers

1. Monitor your accounts regularly using your credit union's online and mobile services, and be on alert for any suspicious activity on your credit union accounts.
2. Notify your credit union immediately if fraudulent charges are suspected. Set up online alerts to receive automatic notifications of account activity.
3. When shopping online, make sure the session with the retailer is secure at the point of checkout. Look for the "https" in the website address before adding any personal or card information.
4. Review your financial statements carefully to make sure all transactions are reconciled. Fraudsters will often make a small purchase to test the waters first. Report any suspicious charges to your credit union right away.
5. If you use your smartphone to shop online, make sure your mobile device is password- or fingerprint-protected.
6. EMV technology can dramatically reduce the potential for card present fraud. Familiarize yourself with its benefits, and use EMV-enabled cards when checking out.
7. Sign up for mobile wallets like Apple Pay, Android Pay and Samsung Pay that use tokenization, which reduces the risk of card not present fraud.
8. Report lost or stolen cards right away.