How to Best Protect Member Data During the Holidays

By Scott Johnston
December 14, 2017 • Reprints

'Tis the season for holiday shopping. Members shopping on sites they're unfamiliar with, payment and loan offers in abundance, heightened volumes of card-not-present transactions, statements that are longer than any other time of the year ... these are a few of fraudsters' favorite things.

According to the National Retail Federation, more than 174 million Americans shopped online and in stores from Thanksgiving Day through Cyber Monday this year, significantly surpassing the predicted estimates of 164 million shoppers. While this spending might be good for the economy, upticks in volumes also attract criminals and fraudsters.

Over the past several years, fraudulent activity has skyrocketed around the holidays, and that trend is only expected to continue. Between stolen or counterfeit cards and fake websites, faulty gift cards and automated bot attacks, consumers have a lot to watch out for, especially when shopping online. Given the increasing popularity of online shopping – more than 58 million people shopped solely online from Thanksgiving through Cyber Monday this year, outnumbering the 51 million who shopped exclusively in stores – this is especially concerning.

As trusted advisors to members, credit unions should identify and share ways to boost member protection. Helping members avoid and respond to fraud strengthens overall member relationships. Credit unions can take measures to better safeguard members and their sensitive information through member education, robust internal security best practices and proper vendor due diligence.

Engage Members How They Want to be Reached

Potential fraud scenarios likely aren't top of mind for the average member as he or she is battling the holiday rush. Because credit unions are more deeply versed on fraud and defensive strategies, they should push reminders and relevant information to their members, including tips and best practices for avoiding fraud scenarios and how to properly respond if something does go awry.

There are several tactics credit unions can deploy to effectively reach a wide variety of members. If a credit union has a regular digital or physical newsletter, for example, that's a solid avenue to share information about fraud threats and ways to combat them. Same goes for a credit union's website – this is a great vehicle for sharing information, as it's something many members will access on a regular basis, especially during a busy shopping season.

Social media also provides a strong opportunity to disseminate information, one that credit unions don't always fully maximize. Social media has gained immense popularity as a preferred method of connecting with brands and gathering news and information for all demographics, especially for younger generations. A survey by The National Retail Federation found that 24% of younger generations are planning to spend more money holiday shopping this year than last year, which indicates that they'll likely also be more vulnerable this season. This susceptibility makes active engagement via Facebook, Twitter and Instagram, especially important to reach this particular audience. Remember, the fraudsters are using these channels to reach your members, too. Incorporating visuals or graphics is an effective way to increase engagement across all platforms.

To specifically target Generation Z, credit unions should consider leveraging video. According to a recent study by AdWeek, 95% of Generation Z regularly uses YouTube. A sharable video explaining tips and tricks for staying secure this holiday season could really resonate with this group.

And, don't forget the branch. Even though branch traffic has generally been declining in recent years, the branch is still a significant point of interaction for many members. Training employees to proactively speak about fraud best practices and prominently displaying pertinent signage and literature can help reach members with a personal touch.

Fortify Internal Security & Properly Vet Vendor Partnerships

While it may sound obvious, another way to make sure credit unions are doing everything they can to protect members is to take a close internal look at institutions' own security practices and protocols. In the age of proliferating cyberattacks, it's likely that credit unions themselves will be the target of hackers at some point, and they must ensure members' sensitive information is well protected with strong firewalls and appropriate data storage.

This also extends to evaluating security levels of a credit union's vendor partners. Credit unions must practice due diligence when teaming up with technology providers that will house members' data. Not all vendors are created equal, so credit unions must hold themselves accountable for thoroughly vetting each potential partner and validating their security controls, certifications and procedures before making a decision. An increasing number of credit unions are even leveraging third parties to help determine security and risk scores for their technology providers to ensure members' data remains in the most secure hands. If something happens and information is compromised because of a vendor, members will ultimately blame the credit union and not the non-member facing partner, damaging member relationships and the credit union's reputation.

By deploying targeted member awareness campaigns, practicing sound internal security and conducting proper due diligence with vendors, credit unions can better safeguard members' sensitive information and funds. Credit unions have an advantage this holiday season because of their strong member relationships and commitments to service. Engaging members about what's being done to protect them and what they can do to protect themselves builds a sense of confidence and trust that may lead to an opportunity for credit unions to gain wallet share, or even become the default card-on-file more often. The greatest gift a credit union can give is the sense of security; its returns can outlast most of the toys under the

Scott Johnston is EVP/COO of Member Driven Technologies. He can be reached at sjohnston@mdtmi.com.