A Holiday Gift to You: New and More Secure Ways to Pay This Holiday Season!

A lot has changed since last year's holiday shopping season when it comes to crossing off your holiday shopping list. For consumers, it's nothing but good news as 2015 is shaping up to become the most secure shopping season on record. Here's what to know when you go to pay, in-store, online and on-the-go.

Chip Cards Leading the Charge against Counterfeit Fraud

As more Americans begin using their chip cards for the first time this holiday season, it's important to know why chip technology makes payments more secure. The chip generates a unique, one-time code for each transaction, adding another layer of protection to every purchase. This technology is virtually impossible to replicate, which means criminals cannot take stolen card information and create counterfeit cards.

Haven't received your new chip card yet? No problem. Whether consumers are paying with a Visa chip or magnetic stripe card, they are still protected by Visa's Zero Liability Policy, which guarantees that consumers won't be held responsible for unauthorized charges made with their account or account information. [1]

Momentum Continues for Chip Cards in the US

- **180.6 million** Visa chip cards have been issued in the US, an increase of **531%** from 2014.*
- **7 out of 10 Americans** now have at least one chip card in their wallet.
- **592,000** merchant locations are chip enabled, a **49% increase** in October 2015 alone.
- The volume of chip transactions in the US increased by **42%** in the last month, from **$4.8B** in September 2015 to **$8.9B** in October 2015.

* As of October 31, 2015

Mobile Payments Reach New Levels of Security

You may be surprised to learn that one of the most secure (and convenient) ways to pay this holiday season is not in your wallet. It's on your phone! Mobile payments, through platforms like Apple Pay, Samsung Pay and Android Pay, are as secure – if not more so – as the credit and debit card experiences consumers have become so accustomed to. This is thanks to tokenization technology, a process largely invisible to the consumer that replaces

[1] Visa's Zero Liability Policy covers US-issued cards and does not apply to certain commercial card transactions or any transactions not processed by Visa. You must notify your financial institution immediately of any unauthorized use. For specific restrictions, limitations and other details, please consult your issuer.

sensitive payment account information (including the 16-digit account number, expiration date and security code) with a unique digital identifier. Mobile payments apps like Apple Pay also use the account holder's fingerprint to authenticate the transaction. This type of biometric authentication is a convenient and secure alternative to signatures or PINs.

Quicker and Safer e-Commerce with Visa Checkout

If you've decided to avoid the mall mayhem this year by taking your shopping online, keep an eye out for the Visa Checkout button, a fast and secure alternative to filling out online form fields. Enrolling your card is simple, and once you've signed up, you can complete your online shopping with a single account on any of your devices. By working with merchants to integrate tokens into Visa Checkout, Visa will be paving the way for its security technology to extend to virtually every type of consumer payment experience – in-store, on-line and in-app.

Three Tips for Preventing Fraud This Holiday Season

1. **Sign up for Transaction Alerts:**
   One of the best ways to identify fraudulent transactions during the holidays is to sign up for email or text "transaction alerts" from your bank. Delivered directly to you via email, SMS text message or through your mobile banking application, alerts let you take immediate action if you believe a potentially fraudulent transaction is taking place. Consumers are still protected under Visa's Zero Liability Policy; however, the sooner you flag these charges to your bank, the quicker it can be resolved.

2. **Keep an eye out for Mobile Location Confirmation:**
   Cardholders at participating financial institutions can register their mobile device's geo-location data to serve as an additional input into Visa's predictive fraud analytics. This means if a transaction is attempted at a store in Tampa, but your smart phone is at home with you in Minneapolis, Visa will flag that transaction as suspicious to the financial institution that issued your card, so they can decide whether to authorize or decline it.

3. **Be vigilant. Protect yourself against phishing, identify theft and other scams:**
   - Only open emails, attachments and links from people you know.
   - Avoid sharing. Don't reveal personal or financial information in an email, text or over the phone.
   - Keep current with your software and virus protection.
   - Create strong passwords.
   - Monitor your account statements closely for unusual activity and report suspicious charges to the financial institution that issued your card.