Protect Your Business from Rising Credit Card Fraud

Despite the efforts of card brands, credit card fraud continues to grow through a variety of methods. The most popular method of fraud appears to be committed through skimming acts. Online sellers have become prime targets for fraud and have experienced a whopping 140% increase in credit card fraud over the past three years.

What Are Skimmers

- Skimmers are card-reading devices inserted into payment terminals to steal card information.
- They are frequently inserted into gas pump readers.
- They use blue-tooth technology to remotely beam the credit card data to the fraudster.
- Data is captured and sold on the black market to be used in online transactions.
- Desktop terminals and gas pumps are the popular places to install a skimmer.

Other Types of Fraud

- Other fraud on the rise includes scams targeting cardholders into providing credit card data.
- Fraudulent Card-Not-Present transactions represent a whopping 65% of all fraud losses.
- Occurs with online transactions, phone payments, and manually entered transactions.
- It costs more when you manually key a transaction because the risk of fraud is higher.

Geographic Data

- Virginia, Texas, New Jersey, Florida, and Colorado have seen fraud increases of 50% or more.
- Virginia and Texas are included in the top five states for compromises.
- California is the top state for skimming.
- The United States, United Kingdom, and Australia are countries with the highest rates of fraud.
- The U.S. accounts for around a third of all global fraud losses.

The Bottom Line

- Stay informed about the latest fraud trends.
- Be vigilant in watching card readers, payment terminals and onsite ATMs for obstructions
- Use contactless Tap N’ Go payment technology.
- Be diligent in who you give your credit card data to over the phone.
- If asked to provide a credit card number over the phone, hang up.

Merchant Tips to Avoid Credit Card Fraud

EMV Chip Technology: Use chip-enabled cards and dip the chip rather than swiping.

Advanced Authentication Methods: Use two-factor authentication (2FA) for online transactions. This adds an extra layer of security by requiring users to provide additional verification beyond just the card number and CVV.

Behavioral Analysis: Be weary of customers who are too friendly in phone orders. If they ask you to run the card right away, this is an attempt to see if the card works and should raise a red flag. Pay attention to those loitering around payment terminals.

Secure Payment Gateways: Use secure payment gateways that encrypt sensitive data in online transactions.

Training: While everything you have read in this article can help you avoid fraud losses, it is important that you also train those who accept payments in your business.

Who is Aurora?

Aurora Payments provides reliable payment solutions for any industry and any environment. As a Full-Service Provider (FSP), we have all the products, services, solutions, and support Merchants need - all-in-one place.

Interested in learning how you can eliminate credit card processing fees?

Send us an email at hello@risewithaurora.com

call us at 833-287-6722

You'll be saving money in no time!