Payment Security Trends: What's Ahead?

As the payment landscape continues to evolve, so do the issues surrounding information security. Here are five payment security trends that will likely have an impact on the payment processing industry.

cardknox
A Fidelity Payments Company

70%

of consumers believe that biometric screening is easier than other identity verification methods.

Biometrics

Passwords will soon be a thing of the past as biometric identity verification becomes more widespread.

Market research studies show that up to 70% of consumers surveyed believe that biometric screening is easier than other identity verification methods, and that 46% of consumers think biometric methods are more secure than PINs or passwords. As payment processing technology continues to improve, expect to see more innovative and user-friendly solutions in the future, such as fingerprint scanners, and voice and facial recognition systems.

Machine Learning and Artificial Intelligence

Millions of pieces of cardholder data and payment card information pass between merchant payment terminals and banks every day all around the world, giving cybercriminals round-the-clock opportunities to intercept that information and commit fraud. With the help of artificial intelligence (AI) technology, more and more banks are using machine learning to "train" their software systems to safeguard cardholder information by scanning transaction information to quickly detect fraudulent activity.

The Internet of Things

Millions of American homes are equipped with digital assistants (smart speakers), video doorbells and security cameras, automated lighting and heating/air conditioning systems, TVs, laptops and tablets, gaming systems, smartphones, and even kitchen appliances, all connected by the Internet of Things (IoT). As more and more make digital purchases using smartphones and other mobile and IoT devices, all that connectivity will require an ever-increasing need for security.

Numerous data breaches have occurred in the United States since 2017, exposing the PII of millions of people.

Account Takeovers and New Account Fraud

An account takeover (ATO) happens when a hacker gains unauthorized access to an account belonging to someone else and uses that information to commit further crimes. Many consumers use the same username and password for multiple accounts, so when a fraudster obtains the login credentials for one website, they can use that information to hack into the consumer's account, or sell the login information on the dark web. Because consumers have become more comfortable storing payment card information online, personal accounts have become a favorite target of cybercriminals.

New account fraud (NAF) occurs when fraudsters obtain personally identifiable information (PII) (such as a person's full name, Social Security Number, birth date and place of birth, and driver's license number), and use that information to open accounts under a fake identity. Numerous data breaches have occurred in the United States since 2017, exposing the PII of millions of people, making NAF the fastest growing form of identity theft today.

PCI Compliance

Payment Card Industry Data Security Standard (PCI DSS) guidelines continue to figure prominently in payment card security trends. System vulnerability scans help identify vulnerabilities and misconfigurations on a merchant's website, and provide valuable information that improves protection against Internet hacking. As technology advances and hackers continue to find new ways to compromise payment processing systems, PCI scan compliance will be even more important for merchants in all industries.

TIP

Ensure your POS system supports EMV chip-card technology.

Staying Ahead of Cybercrime

A lot of what happens online is out of your control, but there are some specific steps you can take to safeguard your business and your customers' cardholder data. You can:

- Ensure your POS system supports EMV chip-card technology.
- Reduce fraud with 3D Secure 2.0 technology to authenticate a customer's identity.
- Integrate tokenization technology to encrypt sensitive cardholder data in card-not-present transactions.
- Establish strong, multi-factor identity authentication procedures for customer accounts to validate customer identity.
- Integrate PCI-ready POS terminals and iFields technology into your system.

If you'd like to learn more about Cardknox and our suite of security tools and services, visit our website.