Security Tips for Retailers

If your business accepts payment cards, it is important to have security steps in place to ensure your customers' information is safe. Your bank or payment services processor can help you prevent fraud. In addition there are free resources and general security tips available to learn how to keep sensitive information—beyond payment information—safe. Below are some quick tips to help get you started:

Know the Who, What, Where of Your Sensitive Data

- Make a list of the type of customer and card information you collect and store—names, addresses, identification information, payment card numbers, bank account details and social security numbers. It's not only card numbers criminals want; they're looking for all types of personal information, especially if it helps them commit identity fraud.
- Ask yourself, where do you keep this information and how is it protected?
- Determine who has access to this data and if they need to have access.

If You Don't Need It, Don't Keep It

- Once you know what information you collect and store, evaluate whether you really need to keep it. Businesses may not realize they're keeping unnecessary data until they conduct an audit. Removing and destroying sensitive data from storage makes it harder for criminals to steal it. Work with your bank or payment processor if you are unsure what data to keep or delete and ask if they have any rules governing data storage that you should be aware of.
- If you've been using card numbers for purposes other than payment transactions, such as a customer loyalty program, ask your merchant processor if you can use tokenization instead. Tokenization is technology that replaces card numbers with an alternate number that can't be used for fraud.

When You Choose Tools or Services, Make Sure They're Secure

- The payments industry maintains lists of hardware and software providers that have been validated against industry security requirements. The list can be accessed through the PCI Council here: https://www.pcisecuritystandards.org/security_standards/index.php
- Visa also maintains a list of service providers that have been validated against industry security requirements. That list can be found here: http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf
- If you outsource your payment application and/or network installation and maintenance, have a conversation with your third-party integrator or reseller about security and ask if the payment software installed is compliant with the latest version of the Payment Application Data Security Standard (PA-DSS).
- Isolate payment systems from other, less secure programs, especially those connected to the Internet. For example, don't use the same computer or point of sale system to process payments and surf the Internet.

- If you use a computer at your business to handle cardholder data or facilitate payment card transactions, make sure you install an anti-virus program and update it regularly. If your business has an outward-facing Internet protocol address (these are Internet-facing entry points to your network), it also is essential to implement a firewall and conduct quarterly vulnerability scans.
- Control or limit access to payment systems to only employees who need access.
- Make sure you implement remote access applications securely or eliminate remote access if you don't need it so that criminals cannot infiltrate your system from the Internet.

Take Advantage of Security Tools and Resources

- Work with your bank or processor and ask about the anti-fraud measures, tools and services you can use to ensure criminals cannot use stolen card information at your business.
- Consider using encryption or tokenization to help secure payment data and minimize its value to data thieves.
- For e-commerce retailers:
    - We recommend that retailers verify the CVV2 code. A CVV2 is the three digit number on the signature panel that can help verify that the customer has physical possession of the card and not just the account number.
    - Retailers can also use Address Verification Service to ensure the cardholder has provided the correct billing address associated with the account.
    - For an additional layer of security, retailers can use services such as Verified by Visa, which prompt the cardholder to enter a personal password confirming their identity.
    - Companies such as CyberSource, a Visa company, can help by providing fraud management solutions and support for online merchants.
- For brick and mortar retailers:
    - Retailers should swipe the card and get an electronic authorization for the transaction.
    - Retailers may also want to consider upgrading their payment terminals to accept EMV chip technology.
        - EMV chip technology introduces unique dynamic values for each transaction, making account data less attractive to steal.

Resources

While small businesses often lack in-house support for securing their customers' payment information, there are a number of online resources that can help:

- Visa's PCI DSS Data Security Compliance Program: www.visa.com/cisp
- Visa's Fraud News blog with information on payment card scams and tips for consumers and small businesses to help stay safe: www.VisaSecuritySense.com
- Visa has worked with the U.S. Chamber of Commerce for several years to educate small businesses in cities across America. The multi-city "Drop the Data" tour is one example of joint educational outreach to help make small businesses aware of the risks associated with retaining prohibited cardholder data. To learn more, visit www.visa.com/dropthedata/index.html

Follow us on Twitter @VisaSecurity

Sign up for Fraud News at www.VisaSecuritySense.com