Preventing data theft and fraud

Data breaches continue to cost companies millions of dollars – in addition to damaging reputations and customer relationships. According to the Identity Theft Resource Center, there were as many as 781 known breaches in 2015, with over 169 million records exposed across business, educational, government and health care sectors\(^1\) – compromising the information for millions of payment cards, passwords, and social security accounts.

Examples of fraud

- **Compromised physical devices**: Skimmers or cameras secretly installed on or near your payment processing equipment to capture customer account numbers and PINs (personal identification numbers).

- **Malware**: “Malicious software” – viruses, worms, Trojan horses, ransomware, and other programs that can be unknowingly picked up when you or your staff use your equipment to browse the Internet and download items from email. Cyber thieves using malware, phishing, and skimmers accounted for 38% of 2015 breaches\(^2\).

- **Employee theft, error, and negligence**: Data theft occurs when employees steal equipment or copy your customer payment information, and use or sell the data to others. About 11% of 2015 data breaches resulted from insider data theft, with employee errors, negligence, or improper disposal of data accounting for nearly 15% of data breaches\(^3\).

Some steps you can take to help prevent data theft

- Upgrade your equipment to EMV chip technology\(^4\)
- Only permit remote access to systems with 2 factor authentication
- Install and maintain a firewall
- Install anti-virus and anti-malware software
- Be sure your software and browser are automatically updated to current versions on a regular basis

(continued)

---


\(^4\) EMV won’t stop a data breach, but stolen EMV data has little value to a fraudster.
Use complex passwords and change them frequently
Use tokenization and point-to-point encryption
Limit employee access to systems during off hours
Restrict and manage access to customer data
Never surf the internet with systems connected to your payment processing systems
Train your staff to watch for signs of suspicious transactions
Review the helpful Visa guide, Reducing Counterfeit Fraud through Acceptance Best Practices

Use strong passwords to protect your system, and change them frequently. We can’t repeat this often enough.

Security experts, including the FBI, recommend passwords with 8 to 10 characters, a combination of upper case, lower case, symbols, and numbers. But most people think complex passwords are hard to remember. Here’s how to create a strong password that’s easy for you.
Use a phrase only you would know. For example: “My son David’s weight is 90 pounds.” Then from this, use the first letter of each word to make a password that is very complex – but simple for you to remember: MsDwi90#s

We’re here to help you
For more information, contact Wells Fargo Dealer Services. Current customers, contact your Commercial Relationship Manager. If you’re not a Wells Fargo Dealer Services Commercial customer yet, call 1-888-937-9997, Monday through Friday, 5:00 a.m. to 7:00 p.m. Pacific Time, and ask to have a Commercial Relationship Manager in your area contact you.

Scam alert: Thieves are trying to get around EMV chip security by inserting their chip cards incorrectly into the slot, so it will seem as if the chip is faulty. Then they may aggressively insist that you manually enter the card information to complete the sale. Try inserting the card properly yourself. If a card is declined, do not insert it again and ask for another form of payment.