Casablanca Ventures

Payments Intelligence

CYBERSECURITY BEST PRACTICES

- Realize that simply placing anti-virus protection on your computers and buying cyber insurance are NOT sufficient protections.
- Redact Social Security numbers except for last four digits, and encrypt if storing digitally.
- Never ask customers to use their SSNs to access online accounts or websites.
- **Communicate!** Tell your customers about precautions your business is taking to protect their personal and credit card information.
- Pay special attention to online orders.
- Google, download, read, share and retain "Visa Acceptance Guidelines for Merchants"
- Don't keep credit card information unnecessarily.
- **Don't slack on compliance.** Ensure all software is updated, PCI-DSS compliant and PA-DSS (Payment Application Data Security Standard) certified.
- **Use end-to-end encryption.**
- **Be vigilant.** Keep detailed records of all sales transactions, including the date, time, contact information for the customer, and names of employees involved in the sale. Detailed notes will become invaluable if a data breach does occur.
- **Act fast.** In the event of a data breach, the key is to determine the cause of the breach and implement solutions as quickly as possible. Your detailed records should help you determine exactly when the breach occurred, allowing you to immediately take action to fix the situation and let affected customers know.
- **Meet PCI DSS standards.** Do not store numbers, but if they must be stored, tokenize them. If necessary, only the last four digits can be stored in clear text. CVV2 code should never be stored in any form. Some states have retention limits for storage.
- **Data disposal/destruction:** Safe disposal of PII (Personal Identifiable Information) is mandatory in 28 states, meaning any PII should be shredded, pulverized, incinerated, etc., including CDs, DVDs and portable USBs. Software should be used to ensure the hard drives are completely erased in old computers, laptops, and smartphones.
- **Data Retention:** Limit retention to no longer than necessary to carry out a business purpose or as legally required. Some states dictate length of retention. The extent of security and storage location for each record should be based on the nature, scope, and risk of theft associated with each record.

- As with the Target breach, many attacks come through vendors, so seek out partners that use strong authentication and adhere to robust data security standards.
- **Administrative Safeguards:**
    - Establish a policy or procedure for each aspect of the business that deals with PII.
    - Minimize access to view or handle PII.
    - Third party or vendor contracts should ensure vendors will have protection for PII in place.
- **Technical Safeguards:** Have a layered approach. No single product will provide a 100% guarantee of security.
- **Physical Safeguards:** Physical security involves multiple layers of independent systems including closed circuit television surveillance, security guards, protective barriers, locks, access control protocols, and many other techniques.
- **Designated Employee:** Many companies, some required by state law, now designate an employee to ensure these requirements are in place, to monitor employee activity and adherence to policies and procedures, as well as provide training. These are often known as data protection officers, data compliance officers, or privacy officers. Having an employee with a certification such as a Certified Information Privacy Professional is preferred.

PROTECTING YOUR PERSONAL DATA

- DO check your account daily when traveling overseas, and at least weekly when at home, to monitor transactions for potential fraud or overcharges.
- DO use debit cards ONLY for cash withdrawals, especially in high-risk locations. Credit cards offer much more fraud protection than debit cards.
- DO leave some of your cards in the hotel safe when traveling so that if your wallet is stolen or your cards stolen or skimmed, you don't lose access to all of your cards.
- DON'T write down your PIN and keep it near your credit or debit card. Instead, use an encrypted password manager on your smartphone and/or computer.
- DON'T shop online while traveling without using security software like a VPN (Virtual Private Network) like Hotspot Shield or others.
- DON'T leave your smartphone unlocked especially if you store passwords or credit cards on it or use it as a mobile wallet.
- DON'T get cash from non-bank ATMs and ATMs in sketchy locations, even in hotel lobbies if the machine is in an out-of-the-way location. These are easy targets for tech-savvy fraudsters to install "skimmers" inside the machine that can read the data on cards run through the ATM's reader.

For more information, contact:

Wynn J. Salisch, ETA CPP
Casablanca Ventures LLC
203-253-7259
Wynn@casablanca-ventures.com