The Top 10 Ways Acquirers Can...

BLOCK THE BREACH

Powered by THE STRAWHECKER GROUP
The Trusted Advisor To The Payments Industry

Data Breaches Happen Frequently	1,054	breaches last year in the U.S. alone
Data Breaches Cost Millions	$5.4M	is the average cost per company
Most Could Have Been Prevented	89%	of breaches analyzed by the Online Trust Alliance could have been avoided with basic controls and best practices
Primary Breach Targets Are Your Merchants	45% / 24% / 9%	Retail / Food & Beverage / Hospitality

- 2013 broke the record (by nearly double) for the most records exposed: 822 million globally
- The recent Target breach ranked only fifth in breach history for total records exposed
- The average breach cost per record was $188 in 2012

78% OF INITIAL INTRUSIONS ARE RATED AS LOW DIFFICULTY

Something can be done to prevent these breaches

BEST PRACTICES

HERE ARE THE TOP 10 THINGS EVERY ACQUIRER CAN DO TO MINIMIZE SECURITY RISKS FOR THEIR OWN OPERATION AS WELL AS THEIR MERCHANT CLIENTS

1 EDUCATION

If your merchants and your employees do not understand the exposure, risk, and the current threats then they will not be prepared to take even basic precautions

- Institute merchant and employee security awareness training
- Offer online resources and education
- Ask for assistance from your processor and sponsor
- A large number of merchant breaches are due to employee behaviors - monitor for habits that pose risks

2 PCI COMPLIANCE

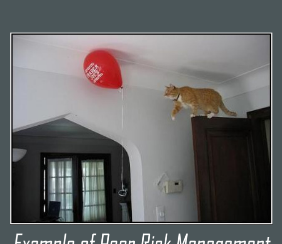
Only **11.1%** of companies* met all demands of DSS 2.0 PCI compliance in 2013

*Merchants, Service Providers, & Other Businesses

Encourage and actively assist your merchants to achieving full PCI compliance & review each merchants SAQ or ROC

2x ONE MAJOR STUDY SHOWS THAT MERCHANTS THAT DO NOT ACHIEVE PCI COMPLIANCE ARE TWICE AS LIKELY TO EXPERIENCE A DATA BREACH

3 RISK ANALYSIS



Example of Poor Risk Management

Complete a Payment Systems Risk Analysis. Every system has risks, you need to understand your vulnerabilities in a rapidly changing environment. Every breached entity believes they are compliant the day before they discover the breach event. Having an objective third party review your security status can help you secure unknown vulnerabilities

4 Strong Passwords

76% of breaches used weak or stolen credentials

Never EVER allow a shared password or use a default credential, and force password expirations for all accounts

Password Tips

- *Don't store passwords electronically or on paper*
- *The longer the better, aim for 6 to 8 characters*
- *It's helpful to mix numbers, letters, specials characters, and upper and lower case letters*
- *Passwords that connect to card information should be changed every 30 days*
- *Try pseudo-random passwords by using the first letter of each word in a personal phrase*

5 Basic Security Tools

↓80% When the European Union migrated to EMV, they enjoyed an 80% reduction in card present fraud

Make sure your merchants are using good defense in depth by using anti-virus and anti-malware tools that are patched and up-to-date. Offer Tokenization, Encryption and EMV products for all POS devices you provide

TOKENIZATION | ENCRYPTION | EMV

6 Contracts

Know what you're liable for!

Be sure that you know your rights, reporting requirements and liability up front relative to any type of data security compromise

7 POS Security

197% McAfee's malware "zoo" had 3.73 million samples at the end of 2013, up 197% from 2012

In addition to teaching your merchants about the need for physically protecting POS devices, it is critical that payment systems have extremely limited Internet access. Merchant employees are often the source of malware from social media sites and normal email

MOST MERCHANTS ARE SMALL, MOST SMALL MERCHANTS AREN'T COMPLIANT, MOST ATTACKS HAPPEN TO SMALL MERCHANTS

77% OF GLOBAL CYBERCRIME TARGETS SMBs

8 BREACH COVERAGE

Only **33%** Only one-third of companies* have data breach insurance coverage

*Retailers, Hospitals, Banks, and Other Businesses

Helpful Link:
Data Breach Security Program FAQs

Offer your merchants breach coverage; would you drive a car without insurance? This can provide an additional revenue stream benefiting both you and your merchants

9 RESPONSE PLAN

83% An estimated 77% of small merchants feel they are safe from a data breach, but 83% of those merchants have no formal written security policy

Prepare a Basic Incident Response Plan – you need to know how to react, what is required by law and who to contact *before* you suspect a breach

10 UNDERSTAND THE LAW

Helpful Links
Data Security and Breach Notification Act of 2013
State Security Breach Notification Laws

State notification laws are complex, vary from state to state and can apply even to single location merchants with out of state customers

IT TAKES AN AVERAGE OF 253 DAYS FOR A COMPANY TO REALIZE IT'S BEEN BREACHED

HERE ARE THREE RESOURCES THAT CAN HELP YOUR COMPANY AND YOUR CLIENTS

(click for more info)

1. ETA's Data Breach Summit
2. The Strawhecker Group's Consulting Services
3. PCI Security Standards Council

ETA ELECTRONIC TRANSACTIONS ASSOCIATION

The Electronic Transactions Association (ETA) is the global trade association representing more than 500 payments and technology companies. ETA members make commerce possible by processing more than $4.5 trillion in purchases in the U.S. and deploying payments innovations to merchants and consumers.

electran.org

THE STRAWHECKER GROUP
The Trusted Advisor To The Payments Industry

The Strawhecker Group (TSG) provides advisory services to maximize client growth and profitability, with its three core services including payments strategy, acquisition services, and payments industry research.

thestrawgroup.com