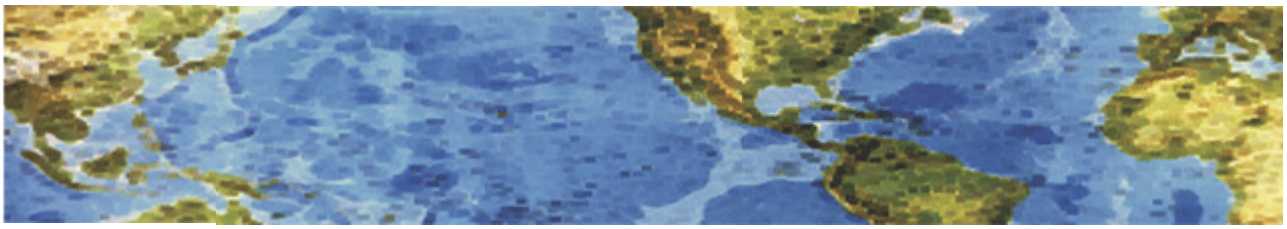
HALL ASSOCIATES



Risk-Based Decision Making Commentary
August 2012 Newsletter

Credit and Debit Card Acceptance Security Standards

The Payment Card Industry Security Standards Council released a set of security standards to be followed by any business accepting credit and debit card payments. Of course, many small business owners are unaware of or out of compliance with these standards. If a small business owner is not able to prove that they are PCI compliant by these standards and there is a data breach, then the small business can be fined for each instance of the breach. The fines can be extremely excessive and for some businesses they could put them out of business.

1. Visit PCIStandards.org and determine your merchant level. The levels of compliance you need to meet depend on how much money you are processing and how you are collecting the data.

2. Identify your validation type. On PCI Standards.org you will find different questionnaires to determine the standards you must meet.

3. Pass a vulnerability scan. If necessary, you may have to implement a vulnerability scan by a vendor to ensure that there are no open areas that can be breached. You must have proof of this scan in order to be compliant.

4. Obtain a certificate of Attestation. Once all else is done, you need to obtain a certificate from the PCI Security Standards Council. This must be done yearly.

And remember, this is an ongoing process. As your credit processing increases or you add new methods of payment your standards will change.

HALL ASSOCIATES

Identity Theft - Children's Identity

Identity thieves are targeting children

It's a crime of opportunity and has usually been committed by someone in the family, but this is changing rapidly. Children are targeted 35 times more than adults, with 15% under the age of 5. This crime tends to go undetected until victims turn 18 and try to get a student or car loan and discover they already have a credit file. All that is required is an SSN, birthday, addresses and parent's names. Since the Social Security verification service can only be used for W-2 reporting purposes, banks verify SSNs, names and birthdates with credit bureaus. So keep your kid's SSNs, birthdates, etc. information close hold, **DON'T** put it on Facebook or MySpace.

Why are children more vulnerable to ID theft than adults?

Because a child's social security number does not have a long credit history attached to it, it is easier for thieves to link it to another name and/or birth date.

How are children's identities getting stolen?

Historically, the most common person was a relative using the child's SSN, now with children spending more time online, thieves use malware and viruses to access necessary information stored on a computer.

What can these identities be used for?

To open credit card and bank accounts, apply for loans, establish utility services, evade taxes, receive government benefits or provide a false identity to law enforcement.

How can this affect my child in the long term?

A compromised identity, even if due to fraud, can be difficult and time-consuming to restore, affecting the child's ability to get credit, college loans, set up accounts and apply for government benefits.