## MY VENDOR HAS SUFFERED A

## DATA BREACH



common theme is not so much IF an organization will be hacked but WHEN it will be hacked. Failed cyber attacks are noted on a daily basis, if not hourly basis, according to many of our industry contacts.

WHAT DOES THIS

**MEAN FOR YOU?** 

DATA BREACH DO NOT

## You need to immediately ensure that your vendors are 1 protecting consumer data and check this on an ongoing

DATA BREACH DO NOT CROSS

consumer level is mitigated.

basis.

Be aware of your state or industry's data breach notification laws and guidance. If you're unfortunate enough to suffer a data breach either from an internal source or third party then you'll need to follow those and, additionally, continue to follow your remediation policy. Regulators are likely

If you experience a data breach, youlre responsible for

remediating to ensure that the risk and future fall out at the

notification requirements set at the State Attorney General level. Most states have now implemented such requirements, so this is an area that you simply cannot bury your head in the sand with the hopes that it goes away. What's a remediation policy? The policy is a response plan to quickly address the data breach and communicate effectively with customers.

to begin looking at this area given the increase in data breach



vendor suffers a data breach?

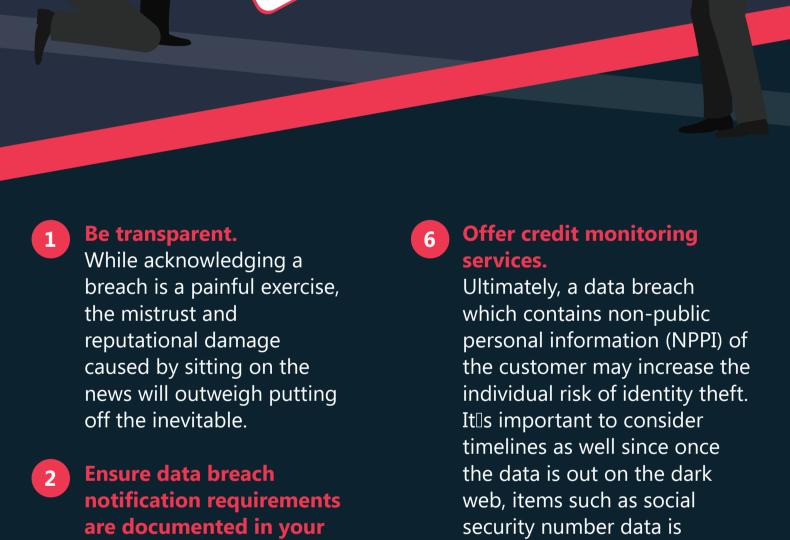
**10 BEST PRACTICES** 

When Handling a Data Breach that Limits the

PERSONAL DATA

So, what do you do if you or your

Impact to Your Brand and Your Customers



7

9

10

may not notify them of a data breach in a timely manner. **Ensure you tell** appropriate people. When required, notify the

and regulator.

breach.

6pm news.

State AG, law enforcement

Define the impact of the

contract language.

shared that there is a

high-level of mistrust

Many organizations have

between third parties who

Understand what you are dealing with. Was the breach isolated to one individual or did it impact many customers? **Adopt a customer** notification process. It's best to notify the impacted customer directly

than have it appear on the

This should be done if customers have access to online tools.

security system.

controls.

vendors.

unlikely to change.

Implement more robust user

authentication procedures.

**Perform root cause analysis** 

Lightening does strike twice.

build a stronger information

**Set expectations with your** 

Learn from this breach and

and enhance security

If the breach originated from the vendor and not your internal organization then perform deep audit testing. If the vendor is unwilling to cooperate then you have larger issues and should reconsider your partnership.

Perform an assessment on

your overall information

Document all updates and

implement refresher training

security processes.

for all employees.

DATA BREACH DO NOT DATA BREACH DO NOT CROSS

The goal of adopting these practices is to be able to document what positive steps your organization has taken to demonstrate how you are managing and being proactive through a risk event. The Equifax data breach of 2017 quickly became a case study of how

a respected organization made missteps in their disclosure process.

After suffering a data breach, you cannot walk away without some

level of damage, so being proactive is your best defense when working





Download free sample assessments of vendor controls and see how Venminder can help you

reduce your third-party risk management workload. **DOWNLOAD NOW**