



Horror Stories: Third Parties Behaving Badly

Awareness is key. There can be a lot to learn by reviewing industry breaches and enforcement actions that other companies have received and been a part of. Within this eBook, we've put together some examples of industry horror stories where organizations were caught doing something wrong.

Read on if you dare...



1

Trick or Treat

Cases of tricking consumers

A small funding firm engaged in deceptive practices in consumer loan offers and received a \$70,000 fine.

This organization said they could provide loans to individuals who were awaiting victim compensation funds in legal settlements, when in actuality the firm served as brokers for others. **They were charged for deceptive consumer lending and lying** about loan costs, the turnaround timeframe to receive loans and even embellishing the truth regarding the size and resources at the firm.

The scary details included that they:

- **Tricked consumers**, as they thought the funding firm was a lender
- Provided **incorrect information about the cost** of loans
- Said they could receive loan funds within an hour but, in reality, **it took much longer**
- Provided **inaccurate information about the company size** and the resources on staff



A financial firm was asked to pay \$700,000 to consumers due to a deceptive healthcare credit enrollment scheme.

Consumers were tricked into believing that a deferred-interest loan product provided by the firm to help them pay for their healthcare needs was interest free. However, interest accrued immediately, and the consumer would be **charged all of the interest** if their balance wasn't paid in full by the time the promotional period ended.

The scary details included that they:

- Took advantage of **distressed patients**
- Taught healthcare providers how to **mislead consumers** about the terms and conditions when assisting them with the application process



2

Are we dealing with vampires who only come out at night?

Cases of no funds and/or poor customer service

Two large prepaid credit and debit card providers received a \$13 million fine.

The providers experienced service breakdowns that put many of their consumers in a difficult spot. Some may even call their experience a “personal financial crisis.” Tens of thousands of consumers were unable to access their money on their reloadable prepaid debit cards in order to pay for necessities (i.e., rent/mortgage, utilities, groceries, etc.). In addition to the issue of unavailable funds, the companies failed to provide customer service during this time and, as you can imagine, many consumers had questions that they wanted answers to, not to mention wanting access to their own money; concerns went unanswered; concerns led to complaints; complaints caught the regulators’ attention and “Boo!” there they were knocking on their door.

The scary details included:

- **Consumers didn’t have access** to their own money
- **Erroneous processing** of deposits and payments
- Consumers were provided with **incorrect account information**
- **No customer service** during a significant service breakdown



A phone company received a \$5 million lawsuit for poor customer service.

A phone company was sued for poor customer service. Upfront, the company offered warranties and assurance that their consumers would be well taken care of; however, when someone needed to take advantage of a warranty, there was a lack of customer service available. Consumers ended up feeling like they were misled.

The scary details included that:

- The company often times **didn't fulfill their warranty obligations**
- They made accessing the customer service team's **contact information very difficult to locate**
- They were **accused of being unfair, immoral** and more



3

Even a magical genie couldn't grant these wishes

Cases of deceptive marketing

A private student loan lender agreed to pay \$23.5 million in consumer relief and \$8 million in civil penalties for engaging in illegal student lending practices.

A student loan lender **engaged in deceptive marketing**. They advertised private student loans at a cost much less than they were.

The scary details included that they:

- Told students a **monthly repayment amount that was wrong**, sometimes as little as \$25, which was unrealistic
- Required students to make **payments greater than what they were initially promised**
- Advertised **incorrect total loan costs**





Credit repair companies agreed to pay more than \$2 million and are banned from doing business in the industry for 5 years because of misleading consumers and charging illegal fees.

The companies **charged advance fees** for credit repair services, even though their fees were illegal. And, they **misled consumers** by falsely promoting their ability to repair credit scores. They said they could remove essentially any negative information and increase consumers' scores significantly. How did they attract consumers and get them to believe them? Deceptive marketing through outlets like sales calls and their websites.

The scary details included:

- Credit repair companies charged **illegal advance fees**
- Offered money-back guarantees, but with lots of **undisclosed limitations**, such as the consumer must make payments for a certain amount of time in order to take advantage of the money-back guarantee
- **Misrepresented** their credit repair services





LOAN

A financial services company was fined \$250,000 and must refund consumers \$255,000 for engaging in deceptive advertising and collections practices.

A payday loans and check-cashing services company misled consumers by producing online advertisements and collection letters that were deceptive.

The scary details included:

- **Deceptive online ads were used** as they ran a promotion that said they'll cash consumer tax refunds for "1.99" when the fee was actually 1.99% of the check amount
- Mailed letters to consumers who were past-due on their loans and said their vehicles could be repossessed if they don't pay, **although it was a lie** since these consumers didn't have loans secured by their vehicles
- **Without preauthorization** from the consumer, the company withdrew money from their bank accounts

PAYDAY




4

It's a spooky sight and a fright for all involved

Cases of exposed data



A data breach that affected over 140 million leads to a \$575 million settlement.



A large creditor agreed to settle a data breach by paying \$575 million and potentially up to \$700 million. Around 147 million consumers' sensitive data were exposed in the breach.

The scary details included:

- **Failure to secure personal information** stored on the network (e.g., social security numbers, addresses, birthdates)
- Within privacy policies, **misleading consumers** regarding strength of their data security program
- Notified of the **insecure network and failed to patch it** after being made aware
- Participating in acts and practices that **caused harm or risk of harm to consumers**
- **Delayed notifying regulators, consumers and others**



**A broker is fined
\$1.5 million for poor
cybersecurity measures.**

A broker failed to implement and enforce proper cybersecurity measures which led to a data breach. Employees weren't monitored or adequately trained on cybersecurity precautions which led to a breach that impacted \$1 million of their consumers' funds when an employee opened a phishing email.

The scary details included:

- **Failure to implement** strong cybersecurity measures
- **Employees weren't trained well** on cybersecurity procedures
- **Didn't disclose the data breach** to consumers in an acceptable timeframe



A third party technology company was sued by their client because of a data breach.

A breach compromised personal information of up to 825,000 consumers. The client says that their third party technology vendor was breached which led to the hacker gaining access to their company information. According to the technology vendor's client, the vendor is guilty of fraud, negligence and breach of contract.

The scary details included:

- The vendor had **insufficient authentication measures and security procedures** in place
- Their password requirements **didn't meet PCI DSS standards**
- The vendor's **employees could share login credentials** and they didn't deploy automatic expirations dates for login credentials
- Utilized **single-factor authentication**
- **And more**




8 STEPS

to Prevent Vendor Risk

Remember, your organization can take proactive steps to help prevent risk and possibly even avoid working with vendors who engage in these practices by implementing steps such as the following:

- 1. Thoroughly vet your third parties** during the vendor selection phase
- 2. Write a breach notification clause into the vendor contract** that requires the third party to notify you of a data breach within an agreed upon timeframe
- 3. Assess the vendor's risk posed to the organization** and determine if the benefits of outsourcing a product/service to them outweigh the risk or not
- 4. Have a subject matter expert (SME) analyze due diligence documentation** such as SOC reports, business continuity planning and disaster recovery plans, cybersecurity plans, etc.
- 5. Regularly request and reassess the most current due diligence documentation**
- 6. Check on the vendor's performance** to ensure they're meeting service level agreements
- 7. Run consumer complaint checks** by scanning sites like the CFPB complaint database, the BBB and complaint websites like ripoffreport.com; also view the UDAAP repository at PaymentLawAdvisor.com and set up Google News alerts
- 8. Always have an exit strategy in place** should you need to suddenly terminate a contract with a vendor for any reason

You have options, and you can prevent engaging in business with a poorly performing or deceptive vendor who may cause you to create your organization's own horror story by simply **doing your due diligence!**



Download free work product samples and see how Venminder can help reduce your vendor management workload.

Download Now



Manage Vendors. Mitigate Risk. **Reduce Workload.**

(270) 506-5140 | venminder.com

About Venminder

Venminder is a leading third party risk management provider dedicated to helping the financial services industry mitigate vendor risk.

Venminder's team of due diligence experts offer a suite of services that can significantly reduce the workload by addressing the tactical challenges of vendor management tasks. Venminder's vendor management software can guide a user through critical processes such as risk assessments, due diligence requirements and task management.

Copyright © 2019 Venminder, Inc.