

August 7, 2007

What complinace looks like: Best practices – phishing

This year's columns have been dedicated to describing this whole thing called compliance. We are now in the process of describing best practices that, if implemented, are designed to help reduce exposure to litigation and regulatory inquiries. Today's topic is phishing.

Background

Yes, I know how to spell. I am not talking about trout or fly here. Rather, I refer to a phenomenon related to identity theft.

The basic scenario is that someone calls your dealership trying to extract personal, non-public information about one of your customers. One of your customers that you already gave a privacy notice to stating that you will safeguard his personal, non-public information. An identity thief casting a line to a receptionist or sales person or billing clerk trying to catch the coveted non-personal, public information.

Examples

One dealer reported that someone called his dealership claiming to be a collector for a collection agency that was skip-tracing the dealer's customer. The dealer had recently sold a car to his customer and the collector wanted the credit application read over the phone under the pretenses that it would help the collection agency collect its debt.

The dealer refused (thank goodness). The collector threatened to send a subpoena for the records and files. The dealer called her bluff.

Three days later an official-looking subpoena showed up in the mail. This dealer's staff was astute enough to escalate the request and accompanying subpoena up the chain for approval. One of the links in the chain noticed that the day and date on the subpoena were inconsistent. In other words, July 20th was not on a Monday. Further investigation with the clerk of courts confirmed that the subpoena was a fake.

The dealer is not sure if the person who sent the subpoena is with a collection agency who just broke all kinds of Fair Debt Collection Act practices or is with an identity theft ring. He is going to let the authorities figure that one out.

Here's another example.

Most of us take summons for jury duty seriously, but enough people skip out on their civic duty, that a new and ominous kind of scam has surfaced. The caller claims to be a jury coordinator. If you protest that you never received a summons for jury duty, the scammer asks you for your Social Security number and date of birth so he or she can verify the information and cancel the arrest warrant. Give out any of this information and bingo; your identity just got stolen. The scam has been reported so far in 11 states, including Oklahoma, Illinois and Colorado. This scam is particularly insidious because they use intimidation over the phone to try to bully people into giving information by pretending they're with the court system.

These are just two examples of the many that I hear showing how creative and unscrupulous identity thieves are.

Best Practices

The Gramm-Leach-Bliley Act and the Safeguards Rule that resulted from the Act requires that a dealer provide employee training. A portion of this training should include the recognition of when



someone is phishing for someone else's personal, non-public information. A portion of this training should include an escalation procedure that employees are to use when they receive these phone calls or requests.

Gil Van Over is the President and founder of gvo3 & Associates, a nationally recognized F&I and Sales compliance consulting firm (www.gvo3.com).

© 2007 by gvo3 Consulting, LLC. All rights reserved.

Published by [Dealer Communications](#)

Copyright © 2007 Horizon Communications Inc.. All rights reserved.

Information in this newsletter is provided by both proprietary and public sources. Dealer Communications makes no claims as to the accuracy of information provided by third party providers.

Powered by [IMN](#)