SHINE BRIGHT

5 KEY PRACTICES FOR PROTECTING CLIENT PII

Busy real estate agents routinely collect financial data and other sensitive documentation from their clients. But it's important to remember with all that information floating around, if something were to get into the hands of an identify thief, it may be all that's needed to drain bank accounts, open sham credit accounts, or go on colossal shopping sprees at the expense of your unsuspecting client.

What is sensitive information, and what must we do to protect it?

Personally Identifiable Information (PII) is any information that can be used to identify, contact, or locate an individual, either by itself or in combination with other easily accessible data. PII may include financial, tax, and employment documentation as well as phone number, email address or Social Security number – exactly the type of information we collect in the course of conducting real estate transactions.

Responsible agents typically don't leave such data lying around in a folder on their desks or on the back seat of their cars – and trustworthy brokerages have extensive PII protocols in place, including encryption, strong passwords, and increasingly paperless transactions.

For the conscientious agent, a sound information security plan can be based on five key practices:

1. TAKE STOCK

Know what you have in your files and in your computer, how it moves through your business cycle, and who has access to it.

2. SCALE DOWN

Keep only what you need. As your transaction moves toward closing, there is no need to hang onto some of the sensitive information you needed to have early on.

3. LOCK IT UP

Be aware of and comply with all of your company's physical and electronic security measures.

4. PITCH IT PROPERLY

Make sure any papers containing sensitive client information are shredded or burned so they cannot be reconstructed. For computer files, use software that can wipe information from the hard drive and prevent restoration.

5. PLAN AHEAD

Because there is no guarantee you will never be hacked, be aware of the documentation your company has place that outlines post-breach procedures.

HELPING YOU SHINE BRIGHT

Powered by Title Resources • www.TitleResources.com •