PROTECT YOUR PLASTIC

As new technologies change the way we pay for things, criminals are keeping pace as they devise ways to separate you from your money. Doing what you can to protect yourself is one part understanding the technology and at least equal portions of vigilance and common sense. Still, we can all benefit from some reminders.

"Phishing" refers to out-of-the-blue e-mails, text messages, or phone calls from superficially legitimate sources, often couched in urgent tones, asking for your credit card or debit card information. The thieves then set up counterfeit cards and run up charges on your accounts. Don't take the bait. You might think that these appeals are too brazen to work, but obviously they work often enough to be a tool in the con artists' toolbox. Follow this rule: Never give out your payment card information in response to an unsolicited communication, no matter its apparent source.

Be careful and attentive when using payment cards at ATMs, shops, and gas stations, and not just because of suspicious-looking characters. The bad guys sometimes steal account information by attaching their own devices over legitimate card readers. Beware of plastic sleeves inside the slot where you swipe a card. Another sign of potential trouble arises when the person you are paying swipes your card on two different devices. One of those swipes may be taking your account information for later fraudulent use.

Don't stick your account statements in the pile of bills to be paid without scanning them closely for discrepancies or suspicious items, such as unauthorized withdrawals. Today you can usually do this online, or even on a mobile phone. Even small bogus transactions are worth reporting to your bank, as thieves sometimes hope to escape the consumer's notice with many small transactions.

Recently, thieves allegedly racked up over $25 million in charges, all in small individual amounts, from hundreds of thousands of cardholders. Let your financial institution know right away if a statement or bill is unusually late. That can signify theft of your information that may

be used to commit fraud.

Periodically review your credit reports from the three major credit bureaus. If an unfamiliar card or transaction shows up, you may already be a victim of identity theft. You get one free report from each of the credit bureaus in a year, so, to maximize your monitoring, get one free report from one of the bureaus every four months.

If you fall prey to the thieves, the federal Truth in Lending Act puts a $50 cap on the consumer's liability for unauthorized charges on a credit card. However, for lost or stolen debit cards and ATM cards, or unauthorized transactions in your checking or savings accounts, the $50 cap is imposed by law *only* if you notify the institution within two business days. Wait longer than that, and the ceiling rises to $500, or even more in some cases. The policies of individual institutions may further limit losses beyond those imposed by statute, so it is a good idea to ask your card issuer about any such limits it uses.

****

Nothing in this article should be construed as legal advice. You must consult with an attorney for the application of the law to your specific circumstances.

R. Michael Shickich is the founder of the Injury Law Firm located in Casper. The focus of his practice is personal injury and wrongful death cases.

The Wyoming State Bar does not certify any lawyer as a specialist or expert. Anyone considering a lawyer should independently investigate the lawyer's credentials and ability, and not rely upon advertisements or self-proclaimed expertise.