GEMMER ASSET MANAGEMENT LLC
LOCAL PARTNER | GLOBAL INVESTING

Advisor Connect

Operations Newsletter

June 2019
Issue No. 14

How to Respond to a Data Breach

Fraud, Identity Theft, Phishing, Hacker, Spoofing, Data Breach... just a few phrases we hope our clients are never a victim of. In the unfortunate event they are, how quickly they respond is critical. Simply customize the attached flyer with your logo and arm your clients with the best steps and timelines to minimize the impact.

Within the first 24 – 48 hours:
· Contact your advisor, Social Security Administration, Federal Trade Commission and IRS.
· Close compromised accounts.
· Run reputable anti-virus/anti-malware/anti-spyware on electronic devices.

Within the first week:
· Contact credit reporting agencies to put a freeze on your social security number.
· Review all financial accounts for suspicious activity. Consider adding a password or pin number.

For the next 30 days to one year:
· Continue monitoring financial accounts.

For a more detailed list of steps and timelines, please refer to the attached flyer.

Ask your Operations Experts

Question: What type of money movement can be eAuthorized by your client?

There are four different types of money movements that we can initiate for client's accounts at Schwab. These transactions can be **Journals**, **MoneyLinks**, **Wires** or **Checks**. If your client is unable to come in and sign a form or is looking for a quicker way to get money into or out of their account, Schwab offers eAuthorization for journals, wires and checks. Please refer to the attached flyer for more specific details on each type of transaction.

Cyber Security Tips

Keeping Up with the Fraudsters

Each day there seems to be a new scheme that pops up to prompt clients into sending funds directly to criminals posing to be seemingly normal people. Aging clients or those with diminished capacity are often targets of the schemes below, however please remember that people of all ages are at risk.

Government Official Impersonation Scam: Often FBI or Secret Service impersonators call stating you owe money. They may threaten arrest or may state that they are aware you are involved in a scam and are trying to help you recoup your money. IRS and Social Security Administration scams are currently active.

Lottery Scams: The Jamaican Lottery is the most successful lottery scam. The customer is typically contacted via the telephone and told they have won a larger sum of money but to collect their prize they need to pay an up front fee or tax. They typically start out friendly but can use aggressive tactics.

Sweetheart and Romance Scams: Internet based scam in which individuals use fake profiles on dating sites and social media to target victims. They establish a romantic relationship and then they request financial assistance.

Grandparent Scam: A senior receives a phone call from an individual posing as their grandchild who is in need of money and does not want to ask their parents. REAL LIFE – this scam was used on a GAM member saying his grandson was in trouble and needed funds ASAP. Thankfully he did not fall for this, but someone who is not in contact with their family might have.

Investment Scams: These scams range from non-existent investment products to penny stocks to high risk investments.