MarketSight

Table of Contents

CadaretGrant
Independent thinking.

Dealing with a Deluge of Information

One of the things we tell our clients is that we will help them sort through the blizzard of investment and economic information that they encounter. We use metaphors like "drinking from a fire hose," or "swimming upstream on the Amazon." No wonder. There really is a huge amount of information, interpretation, and opinion that comes to us every day.

All that stuff is actually good, though. For one thing, even if a client is only superficially aware of the current investment news, good and not-so-good markets are less likely to surprise and distress. Moreover, they are more conscious of the need for the interpretation, explanation, and guidance that we provide. This latter point may be a somewhat cynical perspective that arises from my experience as a salesman, but it is just a fact of life in our world.

So, now, how do we actually do the filtering and sorting that gives us the role that we play? My friend Harold has a discipline that he follows. Harold is a salesman at the core and he is inclined to be a bit less organized than the person who repairs his computer so he needs a process — a procedure — to follow. He first identifies the sources in various fields that he most trusts and respects. There is an economist, for example, that he has developed a deep confidence in. Likewise, there are 3-5 market analysts who have won his attention. He has a few newsletters and research sources (they happen to be Morningstar, Argus, and Value Line) that he admires. And he subscribes to *The Wall Street Journal*, *Barron's,* and one or two other periodicals.

He has, by the way, a strict routine for reading these sources. He reads them for one hour every morning before 9:00 a.m. He reads the table of contents (when there is one) and he is disciplined about not bothering to read interesting (but irrelevant) material. He saves it for recreational reading in the evening.

And, finally, he has a monthly meeting with himself wherein he commits his point of view to paper. It is no more than half a page, typewritten, and designed solely for his own reference, so that he has a consistent point of view. He will not change it readily but rather, he will assemble important data, articles, and insights for consideration during his next monthly summary. He does not want to change his viewpoint based on a single item, such as an employment report or a strong move in the debt market.

Thus, he always is committed to his opinion and he says the same thing to everyone at all times. Harold is quite successful.

Cadaret, Grant & Co., Inc.

One Lincoln Center
Syracuse, New York 13202
T: 315.471.2191
F: 315.475.6550

Regional Office:
200 Valley Road
Mt. Arlington, NJ 07856
T: 973.770.2300
F: 973.770.0223

MarketSight is written monthly by Cadaret, Grant for the exclusive benefit of Cadaret, Grant Advisors. To submit comments or suggestions regarding *MarketSight*, please send an e-mail message to cgmarketing@cadaretgrant.com.

Safeguarding Client Information

We don't typically have time to take precautions to protect ourselves from data breaches or identity theft. Retail stores tend to focus on shop lifters and keeping loyal patrons out of danger with heightened security. However, data breaches at merchandising giants are an unequivocal reminder that we are living in a more digital dependent society.

Sure, many of us choose to stand our ground. We may prefer to receive print bank statements still, boycott online shopping, and by no means participate in social media. We feel confident in this decision to combat the data-centric revolution. But, we have been reminded that simply going grocery shopping or stocking up on holiday items with a debit or credit card potentially places our identity in harms way. According to Experian, 50% of breaches occur through hacking and 40% involve malware. Additionally, Suspicious Activity Reports (SARS) show the most common ways to become a victim of identity theft is through the loss of a purse, wallet, mail theft, and fraudulent address changes.

Suspicious activity that may place client information at risk may include any of the following:

Suspicious documents

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the client presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new account or presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious personal identifying information

- Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
  - The address does not match any address in the consumer report.
  - The Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's death master file.
- Personal identifying information provided by the client is not consistent with other personal identifying information provided. For example, there is a lack of correlation between the SSN range and the date of birth.
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
  - The address or telephone number on an application is the same as the address or telephone number provided on a fraudulent application.
  - The address on an application is fictitious, a mail drop, or a prison.
  - The telephone number is invalid or is associated with a pager or answering machine.
- The SSN provided is the same as that submitted by other persons opening an account or other clients.
- The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other clients opening accounts.
- The person opening the account fails to provide all required personal identifying information on an application or fails to respond to notification that the application is incomplete.
- Personal identifying information provided is not consistent with information that is on file with the financial institution or creditor.
- For financial institutions and creditors that use challenging questions – the person opening the account cannot provide authenticating information beyond what would generally be found in a wallet or consumer report.

Suspicious activity related to, or unusual use of, the account

- A new revolving credit account is used in a

(continued on page 5)

Success by Design
Identity Theft Awareness Tips

Identity theft is real, and everyone needs to be careful to prevent or reduce the chance of this happening. There is no single thing that can be done to prevent identity theft, however one thing is clear — knowledge in the hands of end users is the best place to start. Andy Szymanowski, Cadaret, Grant's internal information technology supervisor, discusses what advisors and clients may want to watch for in everyday computing that can lead to, or prevent, identity theft.

What to watch for:

- Unusual Web site pop-ups or targeted ads.
- Significant increase in the number of spam e-mails.
- Acquaintances receiving spam from an individual's e-mail address.
- E-mail and Web phishing — These e-mail messages try to trick users into divulging confidential information. Typically they appear to come from banks or other popular Web sites such as LinkedIn, Facebook, PayPal, and E-bay. Fraudulent Web sites can be very convincing. Look for HTTPS vs. HTTP in the Web address, typically malicious sites are not HTTPS, which signifies that they are not encrypted.
- When evaluating links in an e-mail message, roll the mouse over links in the e-mail message (don't click) and most programs will show the user what the link goes to (refer to image). Domain names ending in .cn, .br .pl, .ru .it .kr all signify a foreign source. Legitimate links should end in .com, .net, or .org.

What to do if a user suspects or is experiencing problems and general good practices:

- Change passwords, do not use common passwords, and try to include unusual characters.
- Do not leave passwords in easily accessible areas.
- Do not share accounts; more people using an account increases the chances of malicious use.
- Backup data — if issues do occur, this can be critical.
- Periodically run tools that scan for Malware (use MalewareBytes, AdAdware, or other tools).
- Keep computer software up-to-date, especially programs that are used most often or programs that include financial data.
- Check account activity on bank accounts and credit cards.
- Set up alerts on credit cards for spending over certain limits.
- Get a credit report.
- Ask a professional for advice.

Safeguarding Client Information

(continued from page 3)

manner commonly associated with known patterns of fraud. For example:

- The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (for example, electronic equipment or jewelry).
- The customer fails to make the first payment or makes an initial payment, but no subsequent payments.

▲ The account is used in a manner that is not consistent with established patterns of activity on the account. For example:

- Nonpayment when there is no history of late or missed payments.
- A material increase in the use of available credit.
- A material change in purchasing or spending patterns.
- A material change in electronic fund transfer patterns in connection with a deposit account.
- A material change in telephone call patterns in connection with a cell phone account.

▲ An account that has been inactive for a reasonable lengthy period of time is used. Taking into consideration the type of account, expected pattern of usage and other relevant information.

▲ Mail sent to the client is returned repeatedly as undeliverable, although transactions continue to be conducted in connection with the account.

▲ The financial institution or creditor is notified that the client is not receiving paper account statements.

▲ The financial institution or creditor is notified of unauthorized charges of transactions in connection with a client's account.

Cadaret, Grant institutes ongoing training for employees to be mindful of red flags relating to identity theft. Our Compliance and Continuing Education (C/CE) advisor-driven meetings focus on this area as well. Recently, the SEC Regulation S-ID implemented provisions in the Dodd-Frank Act, which amended The Fair and Accurate Credit Transactions Act of 2003 (FACT Act), and directed the SEC (and the CFTC) to adopt rules for identity theft red flags. Moreover, the rule requires specified firms to create a written identity theft prevention program (ITPP) that is designed to identify, detect, and respond to red flags — patterns, practices, or specific activities that could indicate identity theft. Cadaret, Grant is intent on safeguarding client information with comprehensive policies and checkpoint procedures.

Please contact the Compliance Department at 800.288.8601 with questions.

Minute to Learn It
Identity Theft Resources

The Federal Trade Commission offers several identify theft resources on their Web site at www.consumer.ftv.gov. Steps are outlined to inform victims what should be done immediately and to monitor progress. The "What to Do Next" section includes information on extended fraud alerts and credit freezes, repairing credit after identify theft, and how to handle lost or stolen credit, ATM, and debit cards. Information on the signs of identity theft and keeping personal information secure can help protect individuals from becoming victims. Victims should realize fast action is the best way to limit the damage. The Web site offers sample letters and forms to help exercise rights as an identity theft victim, like requesting action from the credit reporting companies and businesses where the theft occured as it relates to the opening of new accounts or tampering of existing accounts.

Cadaret, Grant and Pershing Form Enhancements

Cadaret, Grant is introducing updates to the *New Account Form* and modifications to all other forms to simplify account paperwork. Through advisor feedback, we have taken steps to rename, consolidate, and bundle Cadaret, Grant and Pershing forms for more efficient client account management.

To view an informational Web cast replay, please visit the Cadaret, Grant Web site and click on *Library/Marketing Web cast Replays.*

Compliance Corner

Texting and Instant Messaging

FINRA regulations require member firms to supervise and retain instant messages and text messages in the same manner as written correspondence and e-mail communications. The developing technology of instant messaging and texting does not permit Cadaret, Grant to adequately supervise the electronic messages as required to comply with the FINRA regulations. FINRA has stated that if an adequate supervisory program is not established, then the use of instant messaging and texting must be prohibited. Therefore, Cadaret, Grant has adopted a policy that prohibits the use of instant messaging and texting related to securities business, including internal use within a branch office.

Using a mobile device to send and receive e-mail for business purposes raises the risk of client Personally Identifiable Information (PII) being revealed to unauthorized persons. The risk of loss or theft of a mobile device containing e-mail messages with client names, account numbers or other private data is greater than losing a computer from a home or office environment. Any mobile device used for e-mail purposes should be secured with a password or PIN in such a way that a stranger could never activate the device and read the e-mail messages held on the device.

Additionally, advisors should not store client personally identifiable Information or data on mobile device, including your laptop. Secure protocols such as passwords, encryption technology, and physical security safeguards are necessary to protect client personally identifiable information. Never leave your mobile device, including laptops, in an unsecured location. Refer to a mobile device handbook or vendor support for guidance in making a mobile device safe from unauthorized viewing and use.

Advisors on the Rise Open Enrollment

Cadaret, Grant is accepting registrations for the *Advisors on the Rise* networking and accountability program, which runs from February to November.

In its fourth year, *Advisors on the Rise* is a networking and accountability program designed to work closely with small teams of advisors to create a comprehensive plan for cultivating business and fulfilling advisor goals. Cadaret, Grant Team Coordinators assist advisors with holding themselves accountable by providing personalized support throughout the year and tracking progress each month during networking conference calls.

Advisors will connect via conference call twice per month to share success stories and challenges with fellow peers. The team sets the agenda, with one advisor leading the call each month. Additionally, a Cadaret, Grant Team Coordinator leads a networking call on desired team topics. Industry experts, coaches, and business development resources will host educational conference calls on key topics such as referrals, re-engaging clients, and reaffirming trust in the market.

"Advisors on the Rise allows advisors, whether seasoned or new, to share their business experiences and best practices. The excitement of the new advisors is contagious and keeps us seasoned folks on the forefront of trying new ideas and keeping our practices fresh. For the new advisors, it helps to be mentored in a way, keeps them accountable, and helps to learn the ropes without having to recreate the wheel."
—Top Advisor (three year) participant

Agency Case Study

This month the Agency case study resulted from one advisor's response to her clients' question regarding the financial impact a long-term care event may have on their retirement income. Clearly, a long-term care event can have a profound impact on a couple's finances and the heaviest load is borne by the healthy spouse, as a care provider and ultimately — as the survivor.

This case was difficult because the husband was not healthy enough to qualify for traditional long-term care (LTC) insurance or life insurance. The wife was in good health and was particularly concerned knowing she could live for a number of years after her husband's death. She understood their savings could be depleted by his long-term care and final medical expenses. The advisor recommended the couple purchase a $500,000 guaranteed no-lapse universal life contract with a LTC rider on the wife's life. The following range of possibilities will illustrate the wisdom of the advisor's suggestion.

- If the husband needs help with care, the wife may be able to provide it herself at home.
- If the wife's health suddenly declines and she and her husband require assistance, the $10,000 monthly indemnity-style benefit will allow her to use the funds for her care or her husband's.
- If the wife passes away first, the husband receives a $500,000 income tax-free death benefit which is available should he experience a long term care event, to pay his final medical expenses, or perhaps enhance the legacy for their children.

Each of these scenarios is real and every couple faces the physical and financial risks inherent in the aging process. This advisor provided a financial solution to mitigate some of those risks. Insurance is about leveraging dollars to create a pool of money to be delivered when it is needed the most. More and more, couples are turning to LTC hybrid products to solve their long-term care concerns. Please contact Cadaret, Grant Agency at 800.288.8601 to learn more about the life insurance-LTC hybrid.

Trading Knowledge Nugget

Updated New Account Agreement

The content of Pershing's New Account Agreement and Additional Holder/Participant Information Supplement has been updated to comply with regulatory changes and Account Services updates. The updated forms are available in the *Material Catalog* section of *Resources* in NetX360.

Please contact the Trading Department at 800.288.8601 with questions.

Inside Cadaret, Grant

We have some exciting internal initiatives taking place at Cadaret, Grant.

Internally, we are launching a book drive to benefit Upstate Golisano Children's Hospital. Their mission and vision is to be the location for child health care, health policy, pediatric education, and pediatric research in Upstate New York. They offer a full range of general and specialty pediatric services, in a child-friendly, state-of-the-art facility. The hospital has over 87,000 square feet of space and features all private rooms with bathrooms and child/family-friendly amenities. We'll collect new children's books that will be distributed to new patients when they are admitted to the hospital. The hospital has found that a new book helps children adjust and mitigates their anxiety.

We are also participating in a wellness program sponsored by Excellus, one of our health care partners. The voluntary initiative provides a free health evaluation and confidential personal health score for all Excellus members. Participants will also be able to leverage online educational tools, monthly health Web casts, newsletters, and personal health coaching programs. The initial analysis includes a quick blood test, blood pressure screening, and a brief questionnaire. The goal of the program is to help individuals obtain an accurate gauge of their current health status, and continue tracking and/or improving it throughout the year.