Q2 2012

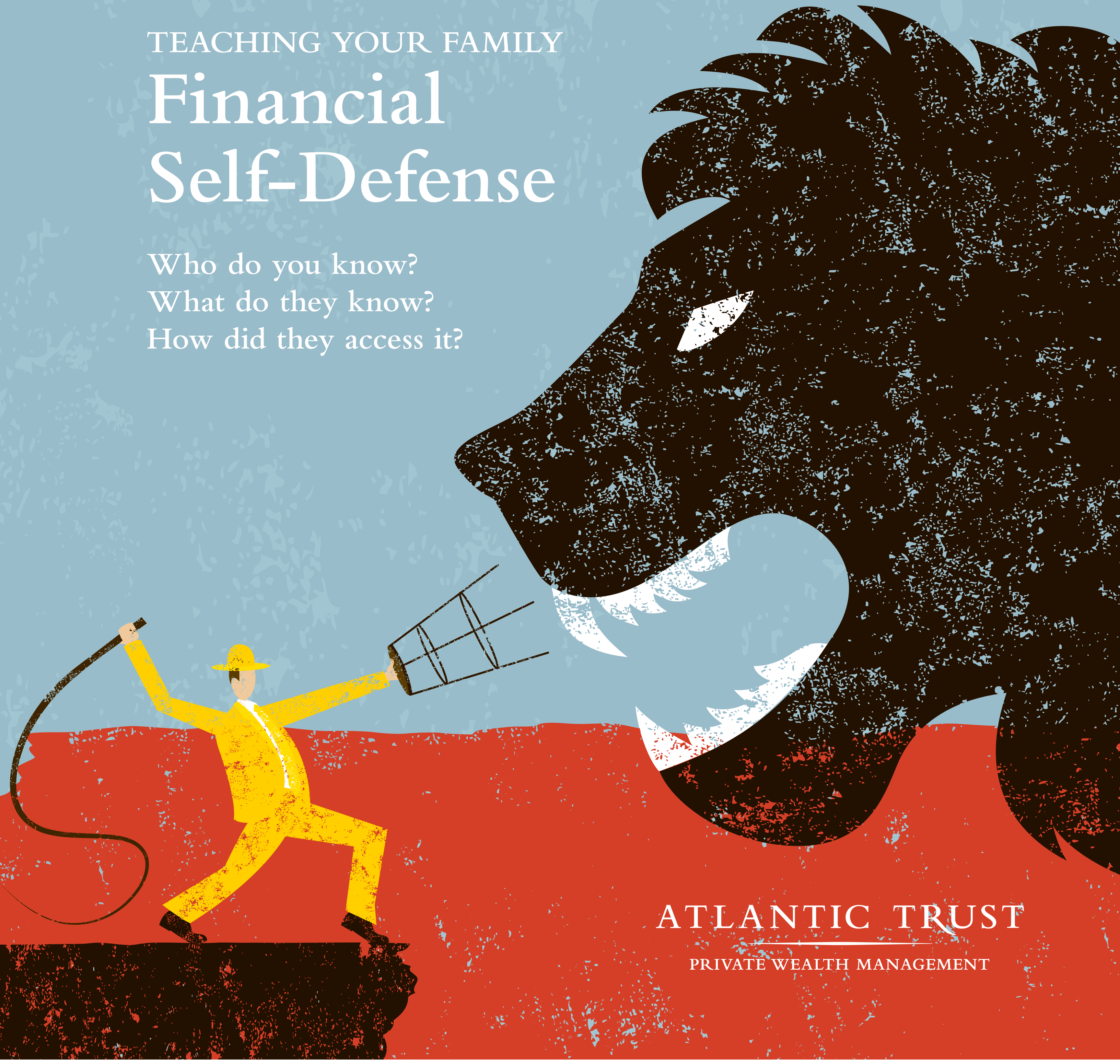
ATLANTIC TRUST

THE ADVISOR

Insights for Integrated Wealth Planning

TEACHING YOUR FAMILY Financial Self-Defense

Who do you know?
What do they know?
How did they access it?



ATLANTIC TRUST
PRIVATE WEALTH MANAGEMENT

"The risk environment today is, in some ways, no different than it has always been—affluent people or those with a high-profile lifestyle can feel like they have

targets on their backs.

What is different, though, is that with social media, people are now willingly opening the door to their lives and saying 'come on in.'"

- John Pullara, Senior Vice President
DeWitt Stern Group

Financial Self-Defense

PART 1
FINANCIAL RISK

Who do you know, what do they know, how did they get access to it, and is that really a picture of your vacation home on your daughter's Facebook page?

THREE BIG AREAS OF RISK

Family risk management includes understanding and acting on three primary areas of risk:

1. *Financial risk:* Threat of exposure to liability, household employment issues and online theft/fraud
2. *Reputation risk:* Threat of damage to reputation and legacy
3. *Personal safety:* Threat of kidnapping or other violent crime

Through our internal expertise and our relationships with outside firms, Atlantic Trust offers clients integrated solutions to comprehensive wealth management needs. Our series of white papers on Family Risk Management discuss the risks, trends and solutions available for affluent families and are accessible on atlantictrust.com. For more information about how we can provide personalized plans for you and your family, please talk with your Atlantic Trust relationship manager.

Safeguarding family wealth means recognizing, acknowledging and, where possible, preventing the risks that can threaten financial security. And those risks can come in many shapes and forms—the 130,000 "open doors" in your computer, the neighbor's teenagers who borrow your jet skis, the subcontractor who "mistakenly" bills you double for work done at your house, the inflated art appraisal. All of these have the potential to damage your financial security and your family wealth—and in large part, all are based on issues of trust.

While the wealthy are often very guarded about whom to trust—especially those with a "sudden money" experience who discover hundreds of long-lost friends—the opposite is also true, according to Teresa Leigh, CEO of Teresa Leigh Household Risk Management. "It is sometimes simply a case of wealthy people being very, very busy and delegating many of the details of their lives," says Leigh. "More important is that the culture of the affluent can lead to feelings of invincibility. On the one hand, a family of significant wealth feels 'shielded' by professional advisors such as lawyers. On the other hand, there is the attitude of 'If I can build and run a successful business, how can my housekeeper harm me?'"

John Pullara, senior vice president at DeWitt Stern Group, agrees that a feeling of invincibility is often present, but points to simple ignorance by many wealthy families. "Risk is a negative topic," says Pullara. "Nobody wants to talk about it. With the guidance of the right advisors, though—the ones who are thinking about what should keep clients up at night—families can protect themselves." Pullara points to a study done several years ago by Chubb that showed most wealthy people are afraid of being caught in a foreign country needing medical attention. "That scenario is easy to insure against," he says. "Where wealthy people are most at financial risk is liability—and its aftermath."

Liability Risk:
Profile, Prominence and Publicness

Pullara's firm goes through a 45-point checklist that assesses a new client's vulnerability to risk. The questions include lifestyle ones such as: Do you have a pool or beach house? Have you just bought a valuable painting or piece of jewelry? Do your children have a nanny? The answers help shape a picture of your profile, prominence and publicness. Unfortunately, deep pockets can be a factor in jury awards in lawsuits—after all, you can't get blood from a stone, as the old saying goes. "The average person is aware of the need to insure for replacement cost of his or her home, but that same person may not think enough about what he or she could be sued for," says Pullara. "And people typically overlook the value of future wages. Let's say you're a 35-year-old hedge fund manager—your future earnings potential is most likely quite significant."

Recent statistics on the exposure that the affluent can face are sobering: In 2011, a Florida court awarded $20 million to the family of a teenager who had been given permission to ride a neighbor's ATV and was killed. In Texas, a jury gave $21 million to the family of a 21-year-old accident victim killed because the defendant was texting while driving. In Illinois, a host liquor liability/negligent supervision case resulted in a $2.5 million award for a teenager paralyzed in an accident after leaving a party supervised by her friend's parents. In many states, if someone is found only 1% responsible for an accident, he or she can be held liable for 100% of the damages to the injured parties.[1]

An exposure that many affluent individuals often overlook is whether they sit on boards of non-profit organizations. Always ask to see the board's directors and officers (D&O) policy, advises Pullara. Many individual umbrella policies provided cover property damage and bodily injury under the non-profit D&O provisions, "but those aren't typically the types of lawsuits brought against non-profit board members," says Pullara. "They're usually breach of duty, discrimination, misappropriation of funds or wrongful termination. Most D&O policies afford defense costs but are included in the policy limit; coverage is shared by all D&Os. Simply divide the policy limit by the number of directors and you may find that liability policy limits are too low at time of loss. You can purchase additional levels of coverage in excess of the D&O policy and the cost will vary depending on what type of organization you're serving and the insurance company. These days, an insurer may view Greenpeace and the local school board in the same risk category."

Pullara says that the risk environment today is, in some ways, no different than it's always been—the affluent or those with a high-profile lifestyle can feel like they have targets on their backs. What is different, though, is that with social media, people of all walks of life are now willingly opening the door to their lives and saying "come on in."

What You Can Do

- *Make sure your P&C coverage keeps pace with any additions such as valuable paintings, antiques or jewelry.*
- *Review any D&O policy under which you're covered; buy excess coverage if you need it.*
- *Be careful about letting non-family members use things such as boats, jet skis, ATVs.*

Online Presence Risk:
Weak Links and Open Doors

Women over the age of 45 make up 24% of individuals on Facebook and the fastest growing demographic group is senior citizens.[2] Are you a woman who uses her full name—first, maiden and married—on social network sites? If so (and it is a way for old friends to find you), you may be giving a clue to somebody with bad intent about the answer to a security question your child may use: mother's maiden name.

Social media has dramatically altered the way people connect with one another—and has given "the forces of darkness," as Roger Dixon calls them, new doors into people's lives. On a typical Facebook profile, others can learn your birthdate, hometown, family members' names and ages, employer, college and if you use location services, "that you're happily posting pictures from another city—and will be 'Home in four days!'" According to Dixon, the chief information security officer for Atlantic Trust and Invesco, adults are guilty of over-sharing (think: pictures of the new grandchildren) but teenage children can be the weakest link. "What teenager isn't tempted to document in real-time his or her trip to your beach home?" While many in the younger generation do set privacy controls on Facebook (or other social media sites), others willingly fill in all the information on their profiles, even though not required. "Unfortunately," says Dixon, "we train people from kindergarten that if there's an empty square, you fill it in. Every piece of information you reveal increases the odds that somebody can know way too much about you and your lifestyle." And sometimes you innocently reveal information to another party you believe to be authentic.

One of those ways is through a classic "phishing" scam. Phishing usually involves the creation of a replica of an existing web page to fool a user into submitting personal, financial or password data. You get an email from what looks like the "real" company—complete with logo—that asks you to click on a link and reset your password because different computers have logged on to your account or there were multiple password failures. As people become more aware of phishing, "vishing" has taken its place—you're asked to call a number with an automated answering service asking for your account information. "This type of fraud is particularly nefarious because it mimics the legitimate ways people interact with financial institutions," says Dixon. "In fact, some vishing doesn't begin with an email. A call comes out of the blue in which the caller already knows your credit card number, increasing the perception of legitimacy, and just asks for the three-digit security code on the card."

Identity theft is still a nasty problem, in large part due to security breaches at big retailers. In 2011, there were 535 reported breaches, exposing the identity information of almost 30.4 million people.[3] Actual identity theft from breaches was about 4 to 6% of exposed records, according to Dixon and the latest numbers from the FBI.[3] While that number may sound low, it's irrelevant if you were a victim of identity theft. But the bigger worry is what could happen in the future. Says Dixon, "The bad guys stealing this information certainly can't use all 30 million records right away—they put the majority on the shelf for later use."

What You Can Do

- *Review your social media privacy settings—and those of your children—and turn off location settings.*
- *Read the privacy policies that you receive from companies that have your personal information.*
- *Remove yourself from online "look-up" companies' databases; search for Google Phonebook Name Removal and remove all your phone listings.*
- *Consider having an information security consultant install your own home-based server.*

Household Risk:
How Wide Is Your Circle's Circle?

Wealthy people who seek to limit the number of casual interactions in their lives to safeguard their privacy often overlook the contacts made with their household by outside vendors. According to Teresa Leigh, during the lifecycle of a large home, an average of 75 subcontractor and vendor companies will work for a homeowner. Add in personal service companies that make house calls and the number likely will exceed 110.

Leigh has more than 28 years of industry experience. Her firm has been educating affluent clients since 2003, providing practical solutions for staffing, household and property management, helping clients identify risk areas within the household and, more often than not, "simply creating order from chaos," says Leigh. The risk areas, and the chaos, can include everything from interviewing, testing and hiring household managers and executive personal assistants to educating clients on state and federal employment law ("It may be your house, but it is their workplace," says Leigh) to auditing art and sculpture appraisals.

Two areas, in particular, can present challenges to wealthy families: those dozens of vendors and subcontractors who can easily plan future high-dollar theft—and the third cousin twice removed from your loved and trusted household manager. In both cases, says Leigh, the risk potential can be high. "It is not that household staff or vendors are inherently manipulative or seeking to harm you, but they have a circle of family and friends, too, and you do not know what pressure they may be under. Your financial risk could begin when an extended family member of one of your household employees starts having financial difficulty, resulting in your employee trying to `help' that family member—just this one time. This situation could expose you or your family to a violent crime, a high-dollar theft, identity theft or a fraudulent service bill."

Like the "open doors" in a computer and the open and uninsured areas of liability, the open spots in household staffing and management are areas of financial risk. "These are generally not cocktail party topics," says Leigh. "But they're very important to responsibly protecting family wealth."

What You Can Do

- *Hire a firm to fully investigate a general contractor you may use at your home and to see if he or she has done background checks on employees and subcontractors.*
- *Create a non-disclosure agreement (NDA) for household staff, please remember that disgruntled employees have the ability to sell or exploit your personal information and an NDA is just a piece of paper.*
- *Consult with a reputable firm, such as Teresa Leigh Household Risk Management, on current employment laws and possible household risk situations. Visit www.teresaleigh.com for more information.*

1 Jury Verdict/Settlement Research, ACE Private Risk Services, 2011, courtesy of DeWitt Stern.
2 "The Demographics of Social Media," Adage.com, May 2011, and the Pew Internet and American Life Project, as of October 2011.
3 Privacy Rights Clearinghouse, "The Top Half Dozen Most Significant Data Breaches in 2011," December 16, 2011.