ATLANTIC TRUST

PRIVATE WEALTH MANAGEMENT

FINANCIAL SELF-DEFENSE

Part 1: Financial Security Risk

How, When and Where You May Be at Risk

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

1. ***Financial risk*** – threat of exposure to liability, household management issues and online theft or 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 wealth management needs. Beginning with **financial risk**, our **series of white papers on family risk management** will discuss the risks, trends and solutions available for affluent families (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.

Risk may come to mind when you think about investments, but not necessarily when you think about your children's nanny, your neighbors using your boat or connecting with old friends on Facebook. All, though, carry the potential to threaten your financial security. Here is what you need to know—and how you can minimize your risk.

Mention the word "security" to a wealthy family, corporate executive, foundation board member or high-profile athlete and the picture that may come to mind is of dark-suited men wearing earpieces. Mention the word "security" to a wealth management professional with a holistic view of a client's total family risk picture, and he or she thinks of actual photos—on Facebook or other social media sites.

Safeguarding family wealth requires recognizing, acknowledging and preventing exposure to risks—and they come in all shapes and forms, including people, computers or legal actions. All have the potential to damage your financial security and your family's wealth, and in large part, all are based on issues of trust. While the affluent are often very guarded about whom to trust—especially those with a "sudden money" experience who soon discover they have 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 the affluent community being very busy and delegating many of the details of their lives to others," 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?'"

In the realm of family risk management, the threats to financial security can come from many places. In general, these threats fall into three main scenarios:

- Failing to consider household or subcontractor help as real "human resources management"
- Creating a situation that could result in a lawsuit
- Leaving too many "doors open" online with social media and other applications

While risk can sound like a negative topic, knowledge about how to minimize risk can help affluent individuals and their families have peace of mind and sleep better at night.

Household Management Exposure: You Are an Employer

Consider the following scenario: A family requires new staff for their multiple households—house managers, an executive personal assistant, a nanny and housekeepers. The hiring process involves finding a good pool of candidates, interviewing them, administering personality and skill testing to selected candidates, and developing a plan to retain staff. Once hired, the responsibilities include staff management, payroll, security procedures and compliance with employment law. Another scenario might involve a multi-generation family's beloved head housekeeper wanting to leave her job after several years of dedicated service and a strong bond with the family. The family is at a loss as to why she wants to leave, so they hire an outside expert who discovers that another member of the staff made unwanted advances toward the housekeeper's underage daughter. The family is briefed on employment best practices and offered an action plan, which results in the family retaining their housekeeper and saving thousands of dollars in turnover costs.

Leigh's firm specializes in management of the affluent household, and she operates in a world where these scenarios happen every day. Leigh stresses that whether it is an estate manager, nanny or elder caregiver, if your family employs household staff, you are an *employer* with legal and ethical obligations. First, keep in mind that although it is your home, it is your employees' *workplace*. "Although your staff may come to feel like members of your family, you can never forget that you have a professional relationship with them," says Leigh. "Being an employer has a set of requirements that go far beyond creating harmony and chemistry, not the least of which is understanding employment law. Knowledge of your requirements and of best practices for hiring will help reduce risk."

Leigh notes that increased restrictions in U.S. immigration laws and work visas have created a greater demand for domestic staff who can work legally in the U.S. As the pool of good candidates continues to dwindle, the number of people who can pass a stringent background and criminal history investigation diminishes exponentially. "On average, we meet with 39 applicants before 1 will pass to the second stage of the interview and vetting process," says Leigh. "That may sound overblown to some people, but let's assume we are talking about a nanny—do you really want to take a chance with your children?" Knowledge about potential risks can also help save money—according to Leigh, household staff turnover is, at a minimum, seven times the employee's annual salary, based on loss of productivity, employer's time, recruiting fees and risk exposure.

Exposure to risk from failing to vet, hire and manage employees properly can come from:

- A lawsuit from a disgruntled former employee
- A claim of sexual harassment or an uncomfortable work environment
- Subcontractors or vendors that have access to your home
- A current employee selling your personal information or gaining unauthorized access to financial accounts
- Failure to monitor invoices from architects, designers, decorators or curators

The latter is unfortunately more common than people may think, says Leigh. Her firm recently helped an affluent entrepreneur who had completed a major renovation of his home. He wondered if he had been overcharged and if he had received authentic items from an art gallery. After auditing the decorator and subcontractor invoices, reviewing documentation on the art purchased and having appraisals of performed, Leigh's firm uncovered a five-figure overcharge and fraudulent records

Best practices: Employing an executive personal assistant

Extremely busy lives, regular travel, a full social calendar, children with their own full calendars. All of these things often lead to the executive personal assistant (PA) playing a key role in the lives of affluent families. That is why it is vital for families to "hire smart," says Teresa Leigh. Below are Leigh's guidelines for harmonious—and risk-free—employment of an executive PA.

1. Hire a professional firm to make reference calls to all past employers prior to hire.
2. Request a credit report on candidates if they will have access to financial information.
3. Hire a professional firm to perform background investigations prior to hire.
4. Insist top candidates take integrity, personality and skill tests prior to hire.
5. Use a system of checks and balances and have a professional bookkeeper reconcile financial accounts to which you give your PA access.
6. If you allow your PA to hire subcontractors, check to make sure that they have a valid tax ID number.
7. Review credit reports regularly to make sure additional credit cards have not been issued by your PA or other staff in your name.

Remember that the IRS looks very unfavorably on those who try to claim household staff as independent contractors; they are not. If you control a person's schedule and and he or she works full-time for you, that person is an employee.

Should you pay your household staff for overtime?

The answer is yes. If household staff members receive a salary, the staff and the employer should keep track of their hours worked and ensure they receive the appropriate overtime pay. The Department of Labor (DOL) considers many household employees non-exempt from the Fair Labor Standards Act, which means they must be compensated for overtime at time-and-one-half their hourly rate. For live-out employees, overtime is more than 40 hours per week, and for live-in employees, it is more than 44 hours per week. Some states, notes Teresa Leigh, have even stricter guidelines for calculating overtime. California, for example, calculates overtime as time over eight hours worked in one day. "And, it is a violation of the law to compensate employees for overtime with time off or gifts in lieu of wages," says Leigh.

Examples Exempt Employees (ineligible for overtime):

- Casual babysitters
- Chefs

Examples Non-exempt Employees (eligible for overtime):

- Day workers
- Housekeepers
- Chauffeurs
- Cooks
- Full-time babysitters
- Nannies

In 2011, the DOL launched a new mobile application for iPhones and iPads specially designed to help hourly workers keep track of their work hours independently from their employers. The app even allows employees to add notes and email a summary of work hours. DOL also offers a printable timesheet for those without iPhones and iPads.

For more information on federal overtime pay provisions and helpful apps, visit www.dol.gov/whd.

for some of the art. In the meantime, the decorator had placed a lien on the home to pressure the client for payment. Teresa Leigh Household Risk Management mediated a successful outcome for the client and retrieved the overcharges paid.

When an affluent family employs household staff, the family can often overlook how far their circle of family, close friends and acquaintances can expand. While most people like to think they take common-sense safeguards to protect their privacy, affluent individuals with multiple residences sometimes fail to consider the number of contacts made with their household by outside vendors. According to Leigh, during the lifecycle of just one 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 will exceed 110. Ask yourself: Are you familiar with all the vendors and contractors that enter your home? If not, you may be placing your family and loved ones at risk. Those dozens of vendors and contractors can easily plan for future high-dollar thefts and present a risk. So can the third cousin twice removed from your trusted household manager. In any case, says Leigh, the risk potential can be uncomfortably 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 may be under pressure. 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 fraudulent service bill, identity theft, a high-dollar theft or a violent crime."

A thorough understanding of the best practices for employing household staff can result in household harmony, well-integrated employees and a significantly lower exposure to financial risk by avoiding the scenarios that can create it. Safeguards in hiring and managing employees are not about assuming the worst about people, says Leigh. "It is about safeguarding families against unnecessary risk."

Liability Exposure: Are You a Lawsuit Waiting to Happen?

According to some experts, the risk environment today is, in some ways, no different than it always has been—affluent families or those with a high-profile lifestyle can feel like they have targets on their backs. To those with unscrupulous motives, the goal of the target is money. But even a lawsuit brought against an affluent family for what appears on the surface to be valid reasons—they were negligent, although unintentionally so, by kindly letting their neighbor's teenagers use their jet skis—can have disastrous financial results.

According to ACE Private Risk Services, the affluent are more likely than ever to be targets of multi-million-dollar lawsuits. 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. 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 and 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.[1]

"The average person is aware of the need to insure for replacement cost of his or her home, but he or she may not think enough about what he or she could be sued for," says John Pullara, senior vice president of DeWitt Stern Group. "And people typically overlook the value of future wages. Let's say you are a 35-year-old hedge fund manager—your future earnings potential is most likely quite significant." Many affluent families are afraid of things such as needing medical care in a foreign

Areas of financial risk when employing household staff:

- Cost of turnover, including loss of productivity, cost of hiring (agency fees, background investigations, relocation expenses, time to interview), imprudent use of employer's valuable time to train and orient a new employee or cost of new security codes/IT passwords
- Breach of confidentiality lawsuits
- Loss of reputation
- Theft of valuables or property
- Identity theft
- Costly employment lawsuits, including wage and hour disputes, discrimination, harassment or wrongful termination

That new community bank wants you on its board ….

Before accepting the invitation, keep in mind the liability risk associated with being a director or officer of a state- or federally-chartered institution. Case in point: from July 2010 through January 2012, the FDIC filed 21 professional liability lawsuits against 178 former directors and officers of failed financial institutions—from large national banks to smaller state-chartered ones—with aggregate damages claimed of $1.98 billion. The allegations included negligence, gross negligence and breach of fiduciary duty. Three cases also named spouses of the directors and officers as defendants. As of January 2012, the FDIC has also authorized more lawsuits—in connection with 44 failed institutions against 391 individuals, claiming damages of more than $7 billion.

Source: www.bankdirector.com

country, a risk that is easy to insure against. Pullara adds, "Many do not realize liability lawsuits pose the greatest risk."

Even if you have tried hard to "hire smart," and then to manage your household staff well, you can be at risk from a lawsuit filed by a former employee if your relationship later sours and you have to terminate the employee. The liability risks from household staff include wrongful termination, discrimination, harassment, untenable working conditions and wage and hour disputes, says Leigh. Lawsuits are not the only risk—damage to public image can also carry financial consequences.

In general, homeowners insurance does not cover these types of claims, because it is designed to cover bodily injury and property damage. An **employment practices liability insurance (EPLI)** policy can provide a broad range of coverage, including wage and hour claims, harassment or discrimination, employment-related defamation and wrongful reference. Many insurers of affluent clients can easily provide EPLI coverage via an endorsement on an umbrella policy with little or no additional underwriting, according to Pullara.

A second big risk that can damage financial security is that of **directors and officers (D&O) liability**. The need for D&O insurance is essential under two scenarios:

1. If you serve on the board of a private company or non-profit group

2. If you own a privately held company and have a board

Lawsuits naming directors and officers are unfortunately quite common today and serving on a board can put your personal assets at risk. According to Pullara, a disturbing trend in non-profit D&O litigation is employment liability, attributable in part to more "informal" management styles often found in non-profit settings. If you serve on the board of a non-profit group—common among influential people who want to act in good faith for an organization or cause they care about—you are subject to personal liability. Always ask to see the board's D&O policy, advises Pullara. Many individual umbrella policies provided cover property damage and bodily injury under the non-profit D&O provisions, "but that is not typically the type of lawsuit brought against non-profit board members," says Pullara. "It is usually breach of duty, discrimination, misappropriation of funds or wrongful termination. Most D&O policies afford defense costs, but they 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 are serving and the insurance company. These days, an insurer may view Greenpeace and the local school board in the same risk category."

If your family owns a **privately held business**, D&O insurance is a must. Because executives and managers of privately held businesses are often involved in many of the day-to-day operations and decisions, directors and officers are more likely to be named in lawsuits. In addition, the personal net worth of owners of privately held businesses is often tied to the fiscal health of the company. A 2011 Towers Watson survey reported that 26% of private companies had a D&O claim of some kind in the last 10 years, while 35% of non-profits did, up from 16% in 2008. The reasons can range from financial mismanagement to misrepresentation of company assets to lack of corporate governance. For private companies, the types of claims included direct shareholder/investor suit, employment-related, fiduciary and regulatory. Of all reported D&O claims from public, private and non-profit entities, 30% involved employment practices.[2] It bears repeating that directors and officers of privately held companies have the same fiduciary obligations to investors

Better safe than sorry: Internet safety resources

These are the basic protections for safety on the Internet:

- Personal firewalls
- Anti-virus software
- Content filtering for protecting children
- Anti-spyware
- Personal encryption

A good resource for content filtering is *FBI: A Parent's Guide to Internet Safety*, which can be found at fbi.gov/stats-services/publications/parent-guide.

For more information and general help on identity theft:

- **Privacy Rights Clearinghouse:** privacyrights.org
- **Identity Theft Resource Center:** idtheftcenter.org
- **Free Credit Report:** annualcreditreport.com
- **Federal Do Not Call Registry:** donotcall.gov
- **Social Security Administration (for reporting theft involving your SSN):** ssa.gov/pubs/idtheft.htm
- **FBI Internet Fraud Complaint Center:** fbi.gov/scams-safety
- **Federal Trade Commission:** ftc.gov/bcp/edu/microsites/idtheft/

In addition, take the time—and show your children how—to understand privacy settings on social networking sites. Finally, when online, especially when viewing a retail site for a purchase, always look for the **https://** (meaning it's a secure site) and/or the padlock symbol on your browser.

and limited partners as do directors and officers at publicly held companies. In the worst case scenario, directors and officers may have to use their own assets to defend themselves in a lawsuit.

Online Exposure: Know Who Has Access to Your Computer

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 4-6% of exposed records, according to the latest numbers from the FBI. While that number may sound low, it is irrelevant if you were a victim of identity theft, says Roger Dixon, chief information security officer for Atlantic Trust and Invesco. But the bigger worry is what could happen in the future. Says Dixon, "The bad guys stealing this information certainly cannot use all 30 million records right away—they put the majority on the shelf for later use."

The "bad guys" are on the minds of people like Dixon, and he thinks they need to be on everyone's mind. For the affluent there is a lot at stake—including the loss of money from online fraud (auction, credit card, escrow services and investment fraud), theft (access to your financial accounts was given to the wrong people) or identity theft (a "new you" is running up credit card bills all over the country). While online risk is not new, Dixon says the more alarming new trend is the intent of some of today's hackers. In the past, a lot of hacking activity could be chalked up to bright but bored teens or young people who got into people's online accounts simply "because they could" and had something to prove. Today, there are numerous criminal enterprises whose sole intent is to gain access and steal information for personal financial gain.

In other cases, the intent is to take over your computer for use in a larger attack. Although, notes Dixon, "They will be happy to take your information if you leave it open." One method of taking over computers is by creating "**botnets**," which can be used by the hacker to attack companies directly or leased in the underground market to spread malware, sometimes used by so-called hacktivists who want to advance a social or political agenda. "An affluent family with a privately-held business needs to be aware of this," says Dixon. "Somebody with a grudge against your company could inflict serious damage this way."

Dixon also advises that everyone should be aware of how new technologies—such as data stored in the vast "cloud" of mobile apps—may or may not be securing information. It is important ask about the privacy and security practices of any outside firm with which you do business. Also, keep in mind that old-fashioned, low-tech crime still occurs, and it is what Dixon calls "**social engineering**." Picture this scenario: You are working on your laptop in an airport waiting area. You are wearing a shirt with the name of your country club on it, or your laptop has your company's name on a sticker. A stranger suddenly strikes up a conversation with you about golf. "I can take what I learn about you just from observation and try to engage you in conversation on a common subject," says Dixon. "From this casual chat, I may be able to learn where you live—'Are you close to your club?'—where you work, what you do, how often you travel, who is left behind when you are gone. If you work in a very large company where you are just a name, I may even be able to convince the person at your IT help desk that I am you and that I need help re-setting my password to access my email—maybe you have just sent an email to a financial institution with your account number included."

"**Phishing**" is another classic online scam but "**vishing**" scams are proliferating. 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

Online risk: Simple steps to improve online security

- Review your social media privacy settings, including 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

what looks like the "real" company—complete with logo—that asks you to click on a link and reset your password because there were multiple login attempts made to your account. Or that the company was unable to process your most recent payment, asking helpfully "Have you recently changed your bank account or credit card?" With "vishing," you may be 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 does not even begin with an email. A call can come 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 back of the card."

Also, be aware of how easy it is to be unprotected on **social media** sites designed for "sharing." On a typical Facebook profile, others can learn your birthdate, hometown, family members' names and ages, employer or college. If you use location-tracking apps, such as Foursquare, others can see "that you are enjoying a meal at a restaurant in another city, and based on your status update—'Home in four days!'—when you are returning home." According to Dixon, adults are guilty of over-sharing (think about those pictures of new grandchildren) but teenage children can be the weakest link. "What teenager is not 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 and other social media sites (often to block parents from picture-viewing), others willingly fill in all the information on their profiles—such as cell phone number—even though it may not be required.

"Take the time—you *and* your children—to sit down and do a total risk evaluation of your online footprint," advises Dixon. "You might be surprised how exposed you are."

1 Jury Verdict/Settlement Research, ACE Private Risk Services, 2011, courtesy of DeWitt Stern.

2 http://www.towerswatson.com/assets/pdf/3790/DandO_Survey_2011.pdf.

3 Privacy Rights Clearinghouse, "The Top Half Dozen Most Significant Data Breaches in 2011," December 16, 2011.

Atlanta 404 881 3400
Chicago 312 368 7700
New York 212 259 3800
Austin 512 651 7800
Denver 720 221 5000
San Francisco 415 433 5844
Baltimore 410 539 4660
Houston 713 214 7640
Washington, D.C. 202 783 4144
Boston 617 357 9600
Newport Beach 949 660 0080
www.atlantictrust.com

ATLANTIC TRUST
PRIVATE WEALTH MANAGEMENT