



How to Create a Family Fortress

|

*6 Critical Action Steps for Keeping
Your Clients Safe at Home, Online, and
On the Road*

BY PAUL JAEB

CONTENTS

01 FORWARD

02 INTRODUCTION

03 THE J2 STORY

04 THE SIX ACTION STEPS

05 THE J2 TEAM

06 THE VALUE OF BEING A TRUSTED
ADVISOR

07 THE MOST IMPORTANT LESSON

FORWARD

Thanks for downloading and reading our guide. I'm Paul Jaeb. I'm known as the "American Private Investigator." I am a partner with my brother, Tom, at a leading private investigative firm based in Minneapolis, MN.

On the day that I received my private investigator's license, which also happened to be my 27th birthday, I ran into my first brick wall. Upon returning to my small apartment in downtown Minneapolis I was greeted with news that the US had just invaded Iraq.

With the economy already suffering from the Savings and Loan crisis, the brief war in the Middle East further eroded consumer confidence and tilted the US economy deeper into the recession. Not a great time to start a business.

Over the ensuing 30 years my team and I have experienced several systemic economic shockwaves. The dot-com bubble bursting and 9/11 hammered dozens of my clients. The slow and painful Great Recession was a four-year reckoning in which many did not recover.

Today, we are faced with perhaps the greatest challenge of our time.

We cater only to high net worth individuals and their advisors. We understand what resources are needed to mitigate against the grave risks that are looming. Families are not only concerned about their loved ones, but also about their investments and assets.

Having led the nation's leading investigative trade association, being an industry thought leader, and travelling the world, I have a unique network of ultra-skilled professional associates. Over the past two months I have spoken to dozens of my contemporaries around the world – and a few things are clear: High net worth families are worried. They want answers and assurances.

J2 Risk Advisors is a highly regarded boutique firm that is uniquely positioned to help you help your clients. While many investigative and security firms abound, very few have the breadth of experience in working with wealthy families.

Our team is composed of licensed investigators, former federal agents, cybersecurity specialists, forensic accountants, and attorneys. As we navigate through this crisis, we would like you to be aware of six resources that are particularly important for you to share with your clients.



INTRODUCTION

A generation ago, families and their advisors had informal local networks they could rely on. If you wanted to know about a new competitor, you might call your uncle. The butcher was a great source for local gossip. As long as you gave to the Police Federation you could rely on the local captain to help out. If someone was threatened, your friends and family had your back.

However, as the economy grew and we expanded our boundaries, these informal safety nets couldn't keep up. Over the past thirty years there has been an explosion of new wealth in the U.S. Wealth Advisors saw this coming before most industries and began to offer services to fill these gaps. Now, you and your colleagues help provide concierge services that reflect this new reality.

J2 Risk Advisors is here to further compliment your offering. I have addressed dozens of client groups over the past ten years with my keynote presentation: "Your Three Biggest Risks: Mitigating Threats at Home, Online, and On the Road."

This guide expands on this work and challenges you to recognize the key threats to the safety and security of your very important clients...and what you can do to help them alleviate these risks.



03

J2 RISK ADVISORS STORY

High-net-worth individuals pose unique needs when it comes to security and risk management. Most of these individuals are active at home, at work, and on the road. Frequent travel, busy schedules, and multiple residential homes only exacerbate the risk.

As an advisor to individuals and executives, you need all the tools and resources available to help your clients mitigate these risks in the most discreet and professional manner possible.

At J2 Risk Advisors, our Family Office and Private Client Services division provides scalable, flexible solutions to address and remediate risk across a wide spectrum.

Whether we are engaging in a proactive assessment or a reactive investigation or security matter, our process is simple and effective:

Assess, Communicate, Remediate, Recommend, and Monitor



Our story: Paul Jaeb and Tom Jaeb are not only brothers, but business partners for over 25 years. Beginning with a desk, a phone, and a fax machine in 1991 they built one of America's most successful investigative firms. After a successful exit, they are back in the game with a much tighter focus – working only with high-net-worth clients and their advisors.

Let's look at some examples of this process in action along with recommendations on specific investigative and security items that, in our experience, go largely ignored.

04

SIX ACTION STEPS



Paul Jaeb



Action Step 1: Cyber - Protect Your Home Network in The New World

Residential cyber security is at the forefront due to the COVID-19 pandemic. Business computers and networks are constantly assessed and hardened to combat security threats.

Unfortunately, home networks are rarely held to the same standards. Residential cyber security has always been a topic of concern for high-net-worth families. The issue is now exacerbated by the fact that executives are working from home over unsecured networks.

Over 37% of J2's customers are already compromised at onboarding.

Over 82% have passwords exposed on the deep/dark web.

Cybercrime to reach \$6T by 2021.

Ransomware and extortion scams continue to escalate at alarming rates.

"Everyday our team witnesses the impacts of high-profile clients whose social media accounts have been taken over, whose home cameras are freely accessible on the Internet, and whose children and family members are subject to cyberstalking, reputational harm, and other types of non-financial damage."

Chris Pierson, J2 Consultant

In recent years cybercriminals have turned their focus to hacking High-Net-Worth Individuals, High-Profile Persons and Corporate Executives. These individuals present easier targets of opportunity for financial crime and reputational loss as they are not protected in their personal lives.

Our team protects the phones, tablets, computers, and homes of our clients using enterprise-grade cybersecurity solutions and our own proprietary technology that discovers weaknesses, protects the individuals, increases their privacy, creates traps for the hackers, and monitors and responds to any cyberthreats that arise.

Our team constantly monitors and reports on the negative impacts of cybercrime on our clients. We see private cameras broadcasting to the Internet, compromised passwords on the Dark Web, devices with no protection, viruses and other malware on devices, and home networks that are vulnerable to attack or already compromised.

Home networks pose unique challenges as individuals and families maintain confidential corporate information and sensitive personal information on the same network and devices. As experts in residential cyber security audits, we follow strict protocols to limit our access to this data while strengthening and protecting the data during the assessment process. When advising your affluent clients, consider presenting these recommendations to them:

- Execute a non-disclosure agreement between the family and the expert to protect sensitive information
- Decide which devices are to be assessed and which are off-limits to ensure that the family is comfortable with the assessment

Action Step 2: Personal Security – Prepare and Be Aware

A comprehensive personal security program for individuals encompasses a broad spectrum, from the initial assessments and general recommendations, all the way to customized training programs.

The most common security programs focus on situational awareness, self-defense training, and communication strategies. These are important and fundamental to the safety and security of high-net-worth individuals.

However, in our experience, there are a few other components that are overlooked far too often.



The Family Emergency Dossier

At onboarding, we ask all our clients the same question: if an emergency occurred and you needed to quickly gather personal information on family members, (e.g., SSNs, DOBs, blood types, etc.) where would you quickly find it?

The answers generally fall into three categories: “we don’t know”, “it’s all over the place”, or “[name] has it but we can’t get a hold of him/her.”

This problem is easily remediated by creating a checklist and following some simple tips:

Aggregate the following general information and maintain it in a secure environment.

- Names, contact numbers and email addresses for your most important advisors and emergency contacts
- Names, contact phone numbers and email addresses for your spouse’s and children’s core friends, co-workers, and family members
- SSNs and DOBs for family members
- Important usernames and passwords
- Scanned images of driver licenses, passports, and recent photos
- Blood types
- Details and instructions on special medical conditions

Maintain an electronic copy in a secure cloud-based environment.

Create contingencies so that outside advisors, friends, or family can access the documents in event of an emergency while maintaining overall security of the documents.

Update the documents monthly.

“She’s just so naïve,” said the mother when I asked her to describe her daughter. “Becky” hadn’t been seen or heard from in almost a week. While she was 22 years old, she hadn’t really been on her own for that long. Moving to Seattle was a big step, one that the mother and father were confident she could handle.

The last message from Becky was a text message when she was in Bozeman, Montana, visiting a college friend. She seemed okay and even sent a photo. That was it.

When adult children go missing, law enforcement is of little help. Since no crime has been reported, they really can’t get overly involved. We knew that this case would be handled by our network of investigators.

The family had shockingly little to go on. Becky told them she had a job with an IT company, was moving to the Madison Park neighborhood, and would be hanging out with a new friend, “Tyler”, who would help her adjust to her new life in Seattle.

With her history of moderate anxiety and prior drug use, we began to speculate that maybe she was in a bad place. “Sometimes her judgment is non-existent”, lamented her father.

Our first step in these types of cases is to aggregate all the personal identifiable information we can. The family of course knew her date of birth and social security number, but they debated endlessly on her height, weight, and even hair color.

They did not know her Twitter handle, even though she was a heavy user. Her brother said that Tyler was a guy, but the mom insisted otherwise. No one knew the new home address or the employer.

With little to go on we moved forward with increasing urgency. Our digital media expert tore into Becky’s social media history. We found her Twitter handle and a new Facebook page. But both went dark over the prior week. We reached out to our licensed investigator in Bozeman to see if she was hospitalized or in jail. Nothing. We checked Missoula, Spokane, and Yakima. Again, nothing.

We decided to assume that she made her way to Seattle. Using the powerful databases at our disposal we developed a list of all “Tyler”s in or around the metro area, between 20-30 years old.

We then researched each one, with an emphasis on those in the tech business. A few fit the profile but were not our person.

However, one of the candidates was a counselor. He specialized in eating disorders and anxiety.

Knowing he would not divulge anything about anything, we surveilled his practice. On the third day, Becky showed up. We interceded.

Becky suffered a setback prior to her trip and transferred her psychiatric care to Tyler. A Tacoma police officer found Becky in a rental car in a Target parking lot. She was unresponsive and was subsequently hospitalized. To her credit, she found her way to her doctor.



Drug Awareness

All families, especially those with tweens and teens, are exposed to the availability of illicit and prescription drugs more than at any time in our country's history.

The issue of drug use is a sensitive one and not easy to address, whether it is advisor-to-family or family-to-children. As a resource to our clients, our approach is to provide timely information and updates on threats that are emerging in this murky underworld.

We don't offer "scared straight" meetings. Rather, we provide a quarterly newsletter that outlines emerging trends, new risks, and factual data and recommendations that our clients can utilize to structure meaningful conversations on the topic and mitigate risk.

Our experts are also available on an as-needed basis to answer questions and provide advice during unique situations.

If you overhear kids talking about Red Bull, Hello Kitty, or Skype, it may not be as innocent as you think. The following were tested recently at a lab in Los Angeles, as a public service:



Sold As: Hello Kitty
Content: 385mg of MDMA (Ecstasy)
Found: Online
Tested: March 9, 2020



Sold As: Skype
Content: 496mg MDMA (Ecstasy)
Found: Bern, Switzerland
Tested: February 23, 2020



Sold As: Red Bull, Red Buli
Content: 400mg of MDMA (Ecstasy)
Found: Online
Tested: April 8, 2020



Action Step 3 : Relationships – Eliminate Risks in Professional and Personal Interactions

We refer to the process of vetting counterparties in both commercial and personal transactions as “Relationship Due Diligence.”

We typically break this down into two categories: professional relationships and personal relationships.

In a corporate setting, high-net-worth individuals and related entities may choose to conduct due diligence background checks related to investments. This is very common but, in our experience, such due diligence is usually only conducted by the buyer on the seller in a standard equity investment scenario.

We advise our high-net-worth clients to consider conducting due diligence whenever they are engaging in a potential business transaction. This could include checking out brokers, counterparties, investment partners, vendors, suppliers, etc.

Regarding personal relationships, rich clients are especially vulnerable. Due diligence on those entities and individuals that are swirling around their daily lives are especially important.

This should include routine background checks on the following:

- Professional advisors
- Home maintenance workers
- Anyone working with or near your children: babysitters, nannies, coaches, and counselors

Just recently...

In a recent example, we were retained by a business that was seeking investors for a rapid growth initiative. A broker brought an international investor to the table. The broker claimed to have conducted a thorough vetting of the investor prior to the introduction.

Our client asked us to conduct a standard background check, just to be safe. Our investigation determined that the investor had been previously indicted in U.S. District Court for fraud and had fled the U.S. after being deemed a fugitive from justice.

Action Step 4 : Self-Assess and Remediate Your Family's Data Footprint

Relationship Due Diligence is common and well known to high-net-worth individuals. Simply put, the process involves gathering information and intelligence on other entities and individuals in order to make informed decisions.

However, most high-net-worth individuals have not considered reviewing the information that is available on themselves. We refer to this self-check process as "Self Due Diligence." This process is largely ignored during most personal security assessments.

Every minute of every day, data is being collected on individual consumers. This information becomes available in open source public records, deep web sources, dark web sources, and through third-party, private database companies that aggregate information from thousands of sources.

This data is used by lenders and investors, employers, insurance companies, governmental agencies, and credit bureaus in order to make informed decisions about consumers. It's also used by criminals to steal identities and perpetrate fraud. In addition to the sources listed above, most consumers are completely unaware that additional companies are aggregating information on their insurance claims history, medical records, social media activity, and spending habits.

These data aggregators are known as "Specialty Consumer Reporting Agencies". Credit bureaus such as Equifax, Trans Union and Experian are examples of standard "Consumer Reporting Agencies".

They collect data on your credit history,

organize it into a database and sell it to lenders and financing companies.

Specialty Consumer Reporting Agencies do the same thing, but they collect information that can have a significant bearing on your reputation, employment, insurance, and other significant aspects of your life.

Most individuals do not know that the content of these reports is available for review. If information is erroneous, a dispute process is available to rectify the erroneous information.

These database companies also aggregate information from social media activity and spending habits. While this information may not have a similar bearing on your credit, employment, or insurance, the information is starting to be used by background screening companies for a variety of reasons.

Employment history records are often aggregated by third-party database companies. When you apply for a job, the background screening company will log into these databases to confirm the accuracy of your previous dates of employment and title. In our experience, these databases are all too often erroneous or outdated. This leads to incorrect information being reported to the employer, which makes the candidate appear to have provided fraudulent information on their resume or CV. This can be mitigated by conducting a self-check prior to completing job applications and finalizing resumes.

Many job seekers are unaware of the actual status of previous civil litigation or criminal records which reference them. In many cases, they believe that certain cases have been expunged or dismissed when the public record reflects otherwise. This can lead to awkward situations. Again, this can be mitigated by conducting self due diligence.



In our experience, many wealthy individuals were unaware that personal identifying information on them and their families was available through simple Google searches. Some of this information can be removed through proper procedures.

Conducting a thorough self-check involves multiple layers of research, some of which are not available to the general public. The following grid contains an overview of the types of information sources that should be accessed, at a minimum.

Upon conclusion of such an investigation, individuals will be able to identify erroneous information which could affect their personal and professional reputations as well as identify personal security threats. Some of this information can then be disputed and remediated, or otherwise removed, from public access.

Public Records

Federal, state, and local lawsuits, liens, judgments, financing instruments, criminal convictions, criminal arrests, bankruptcies, police activity, property ownership, vehicle registration, drive licenses, corporate affiliations, and shareholder references, among other things.

Open Source

Social media platform, blog platform, and general internet references – commonly known as the Clear Web.

Specialty Consumer

Reporting Agencies

Reports containing your information - similar to credit bureaus. These companies collect information on your employment history, insurance claims history, medical records, public records, spending habits, social media activity, etc.

Deep and Dark Web

Internet references that can be found by enhanced research but are not indexed through common search engines - typically anything behind a paywall or requiring sign-in credentials. The “dark” web is a subset that is intentionally hidden – typically a marketplace for illicit activity including the exchange of stolen data.



Action Step 5: Travel – All Security is Local

High-profile persons and executives are typically experienced at international travel and receive advice from experts and corporate security departments. But family units are not always receiving the same training.

A comprehensive travel advisory training program typically contains the following high-level components:

- Situational awareness training
- Pre-planning based upon specific destinations and travel plans
- Training and recommendations from local agents providing information on local customs and security risks
- Flight, hotel, and ground transportation security

In our experience, the most important aspect of travel security is the “Bat Phone”. Individuals and families should be prepared to have a local security expert on call.

These are typically vetted, licensed and insured security experts with knowledge of the local area and contacts at relevant local law enforcement agencies. Here are a few tips on setting up this relationship:

Travelers should have the contact information for their local security expert saved in all their mobile devices. This includes cell phone numbers, email addresses, and office numbers.

The local security expert should also provide contact information for a backup agent.

Travelers should test their mobile device coverage upon arriving at their destination, including the ability to place local and international calls as well as local and international text messages.

Travelers should download and test alternative messaging applications such as WhatsApp, Facebook Messenger, Snapchat, etc. upon arriving at their destination in the event that mobile calling or standard SMS and iMessage tools are not available.



From the Archives

The Story of Jen Le

Jen Le, by all accounts, was a bright and accomplished 17-year-old. She loved to travel with her family, particularly when they went to see relatives in Asia.

While her parents were confident she could handle herself on the mission trip to South America, I wasn't so sure. It's quite different flying into Tokyo than Bogota and VERY different when walking the streets. Her indifference to me and my message was not subtle.

Nonetheless we embedded in her phone the number of our security provider and told her to call her if anything remotely uncomfortable occurred.

We had already vetted the adults who were travelling with the 26 high school seniors and conducted a security audit of the youth hostel that was hosting them. I was guaranteed that the students would not have free time to explore the city. But we prepare for all contingencies.

On their third day in Columbia, Jen Le and her friend decided that there would be no harm in taking a taxi to the flea market that they saw on the way into the city. Although she will never admit it, they knew they made a grave mistake.

After getting lost in the sea of counterfeit purses, belts, and shoes, they found themselves locked in a maze of vendors that got seedier the deeper they went in. Unable to communicate, they began to panic when they noticed several young men following them.

Jen Le remembered the speed dial I placed in her phone. Despite a weak signal, our agent arrived in less than 15 minutes.

Action Step 6: Residential Security – Think Beyond Gates, Guards, and alarms

“Your biggest risk at home is encountering someone already in your house. It’s your highest risk of physical harm.”

-Paul Jaeb, Managing Director



Your clients are no stranger to residential security. From gates to alarm systems to cameras, most high-net-worth clients have physical controls in place to mitigate risk. These controls, if properly managed and deployed, provide security against common risks of theft, intrusion, etc.

In our experience, residential security assessments focus almost exclusively on these physical controls. A comprehensive residential security assessment should also take into account the potential threats that are typically invited into the home (e.g., home maintenance workers, nannies, babysitters, etc.) and the people who live nearby in the neighborhood.

While most of our clients were found to have satisfactory physical controls in place upon onboarding, we have typically advised the following after completing an initial assessment:

- Set up access to local police crime data reports and sex offender registry updates. Review these on a weekly basis to stay abreast of local risks.
- Conduct background checks on individuals who have routine access to your home or routine access to your family members and update these checks periodically.



A

s private investigators and consultants to hundreds of financial advisors, C-level executives, lawyers, bankers, and high-net-worth families, we have an interesting perch in which to view the world.

About half of our business is preventive due diligence (who are the other parties in our deal?) and the remaining is reactionary (who's my daughter dating?).

Most of the time our clients view the world through a very practical lens. They understand when they need advice and are happy to pay for it.

In times of crisis, they often keep their pragmatism. They do so because they have developed great habits. They practice what I call "pragmatic paranoia."

They know that it is wise to always conduct the necessary due diligence, keep track of their reputation, audit their physical security, and be aware of the risks to their children.

However, if your clients do not possess these good habits, these times can bring out a lot of anxiety. Many of our clients came to us initially during a time of upheaval. It could be personal (internal fraud, divorce, missing kid) or could be a force majeure.

What is Opportunity Intelligence?

Simply put, it is researching unique and timely opportunities that are typically off-market.

"I'd like to identify 20-30 motels in the Midwest, to add to our portfolio." -New York Family Office

"A ton of talent just hit the market. How quickly can we background our top candidates?" -Denver Multi-Family Office

"My clients are very concerned about their holdings in the Caribbean. How fast can you get boots on the ground?" -Minneapolis Wealth Advisor

"This is a great time to let your clients know that you have the tools to get them through the unique risks that are present today. As a fiduciary you hold a position of trust. Your clients look to you for guidance, particularly when there are so many unknowns. Opportunities and risks flourish surrounding events like a global pandemic. What happens if your clients miss out on opportunities...or fall prey to the risks?"



-Paul Jaeb



05

THE J2 TEAM



LICENSED INVESTIGATORS
DOMESTIC & INTERNATIONAL

ATTORNEYS
LIC. MN & DC

FRAUD EXAMINERS
CPAS & CFES

CERTIFICATIONS

Certified International Investigators (CII)
Certified Protection Professionals (CPP)
Executive Protection Certifications (ASIS)
Certified Fraud Examiners (CFE)
Certified Public Accountants (CPA)
Certified Financial Investigators (CFI)
Certified Identity Theft Risk Management Specialists (CITRMS)
Certified Drug Recognition Experts (DRE)
Licensed Attorneys
Licensed Private Investigators
Licensed Security Agents

OUR EXPERTS

Former FBI Special Agent
Former Technically Trained Agent (TTA)
Former DEA Special Agent
Former Military Intelligence Officer
Technical Surveillance Countermeasures (TSCM) Expert
Former Chief Security Officer for \$10B Healthcare Concern
Former President of the National Association of Legal Investigators
Former Chief Information Security Officer
Former Chief Privacy Officer for \$50M Technology Company

06

The Value of Being a Trusted Advisor

You are valued by your clients because they can trust you. As trusted advisors who specialize in helping you and your clients sleep well at night, we pride ourselves on anticipating your needs.

If you take nothing else from reading our guide, please remember the one universal truth that drives our entire ethos as private investigators ...

“Those with the best intel always win.”

In the mid 1990's our firm was engaged to conduct an investigation on behalf of a family concerned with the assets of their deceased parents. Their parents were very successful entrepreneurs, having built a large regional retailer.

The firm was extremely generous to the communities they served. Always donating to charitable causes, sponsoring little league teams, and leading trade groups. Politicians often looked to them to lead local initiatives.

The children, now clients, learned from their parents how to be leaders in their own right. Two of them traveled the world providing minor surgeries for underserved people in Africa. Another child ran a non-profit that built affordable housing.

A family trust was established in the early 1980's and managed by a dear family friend (a lawyer). In 1990 the retailer was sold, and the trust received \$45,000,000. Each child began receiving dividends from the trust, with a significant payout upon the death of either parent.

Since the children were not involved in the business and enjoyed little understanding of the trust, they paid little attention. The parents died within months of each other in 1993.

When their lawyer called me to get our firm involved, I remember being stunned that \$45,000,000 could disappear so quickly.

In short order, we uncovered an unsophisticated fraud scheme that had been underfoot for decades. The \$45,000,000 was diverted to seven entities around the globe and virtually unrecoverable.

Unfortunately, the children and their advisors did not **Assess, Communicate, Remediate. Recommend, or Monitor** at all during the preceding years.

Simple due diligence, robust controls, and monitoring would have saved them.

This case was the one that led me into working exclusively with advisors who manage wealth – we don't want to see good people taken advantage of by fraudsters. Our firm has conducted over 100,000 high-level background investigations and stopped thousands of dirt balls in their tracks. We've been serving professionals like you and wealthy families since 1995.

We look forward to meeting you before you need us!



07

THE MOST IMPORTANT LESSON

The fundamental reason we wrote this guide for professionals like you is to help you to remember, “those with the best intel always win.”

The good news for our business is bad news for wealthy, successful people who fall victim to fraud, crime, and find their lives or families suddenly at risk. As trusted private investigative professionals, it's our job to help our clients think ahead, be aware of their blind spots, and help them sleep well at night knowing their family fortress has been well constructed by professionals like you.

Tragically, we were in the living room of Dylan Klebold's family the day he terrorized Columbine High School. We worked for the Ramsey family during the death investigation of their daughter Jon Benet. When the Interstate 35W bridge collapsed, we were the first investigators on the scene.

In our business, we routinely see death, mayhem, fraud, and greed. At the end of the day everything we've investigated could have been stopped or mitigated with better intel. Everything.

Thank You

We hope you have enjoyed reading our guide. We wrote this specifically for family office leaders, trusted wealth, tax, and legal advisors who serve the top 12% of America's wealthiest families.

Those with the best intel always win. Always.™

J 2 R I S K A D V I S O R S . C O M

CONFIDENTIAL INQUIRIES: tom.jaeb@J2riskadvisors.com