Family Wealth Security Risks

Solutions for Families, Family Offices and Family Enterprises

INTRODUCTION

CONTENTS

Families of wealth and business-owning families face security risks in their everyday lives. Many report that privacy and security of personal and financial data is a concern, yet few report confidence that these risks have been mitigated.

Family wealth and activities (business, personal and online) expose families to targeted criminal activity. Multiple family members, households and generations increase the complexity and risk to the family's security and reputation.

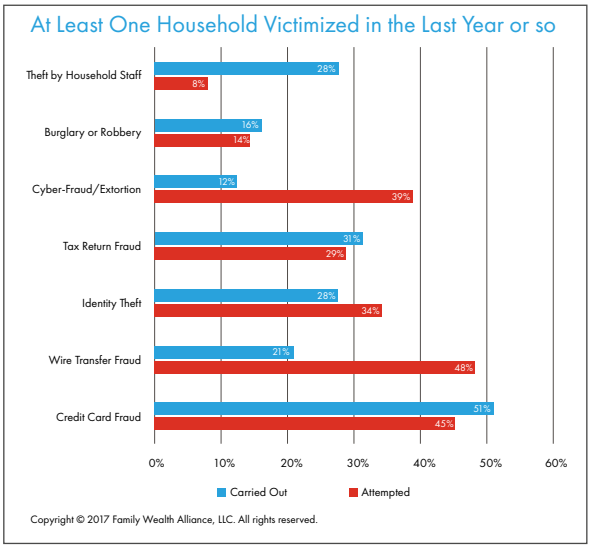
THE THREAT IS GROWING

In the Second Annual Security Study of 55 family wealth firms*, The Family Wealth Alliance found that 73% reported the frequency of security threat incidents have increased over the prior year. Those surveyed reported that in the last year or so at least one client household was victimized.

Top five household attempts reported:

1. Credit card fraud attempts were reported by nearly half of the respondents, with over 50% of incidents being carried out.
2. Wire transfer fraud is highest in failed attempts, and fifth in those carried out.
3. Identity theft failed attempts exceed carried out incidents (tied for third highest).
4. Tax return fraud failed attempts exceed carried out incidents (second highest).
5. Cyber fraud/extortion failed attempts were three times greater than those carried out.

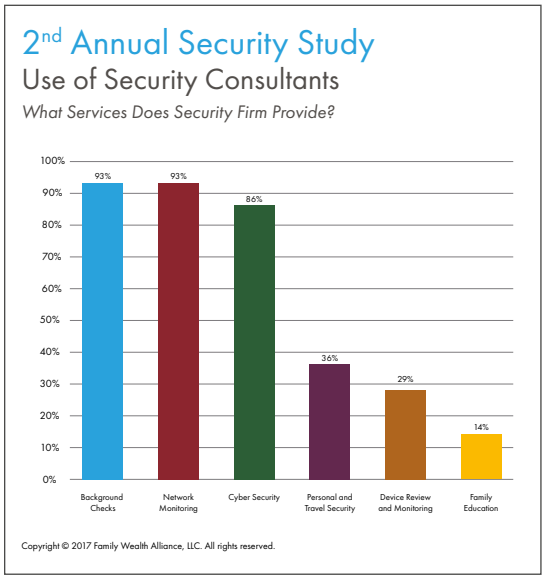
Theft by household staff reported by more than a third with incidents carried out 3.5 times the rate of failed attempts.



THE CLIENT NEED EXISTS

While incident rates have increased, most firms do not offer security awareness education and training or risk-assessment services to their client families. There are client requests for additional security related services with SFOs reporting the greatest demand at 47%.

- Use of security consultants is low and has decreased three points since 2012 (27% vs. 30%).
- Of the services provided by security consultants, the lowest frequency and greatest opportunity are:
  1. Family education
  2. Device review & monitoring
  3. Personal and travel security
  4. Background checks on household staff



In business-owning families, everything is interrelated. Personal and business risks are often blended and are typically managed by different people and processes. This creates a gap in identifying risks and solutions that can be addressed through a holistic and collaborative risk management approach.

The following case study is not uncommon and serves as an example of blended risks facing business owning families and executives. Pro-active planning is the first step in addressing these risks and concerns.

CASE STUDY

Concerns

An executive of a family owned enterprise was targeted in an extortion plot in which the release of private information about members of the executive's family was threatened.

The information had been gathered through following family member posts on social media sites and from phishing attacks on email accounts that revealed sensitive information. The information gathered created unforeseen risks to the following:

- Family privacy and reputation
- Business reputation and brand damage
- Permanency of most online activity
- Financial costs

Lessons Learned

We live in a digital world. Technology makes life easier, and also introduces risk. Security experts tell us that balancing a family's risk tolerance with the intrusion tolerance of each member is critical in ensuring a successful security strategy. As technology quickly evolves, so do the threats. It is important that this be actively managed and not be a once and done activity. Lessons learned from most security threat incidents are more about people and processes than the technology itself.

This whitepaper was written to help families, family offices, and family enterprises integrate a security strategy in a code of conduct framework for family members, business enterprises and/or their family offices.

The sources consulted are listed in the Reference section of the report along with Additional Resources in the Appendix. The information contained in this document is not all-inclusive, nor intended as a substitute for the expert consultation of security professionals.

EXECUTIVE SUMMARY

"IF YOU'VE SEEN ONE FAMILY OFFICE, YOU'VE SEEN ONE FAMILY OFFICE."

This saying extends to the families and their businesses. To honor the uniqueness of each family, business enterprise and/or family office, a framework is offered to help develop a code of conduct that is responsive to the family's risk and intrusion tolerance.

The code of conduct framework includes Objectives (Why), Approach/Process (Who & How) and Structure (What). It is recommended that each family validate the proposed framework and modify for their particular circumstances.

> "Develop a code of conduct that is responsive to the family's risk and intrusion tolerance."

Best practices in cyber, social media, travel and physical security are intended to avoid and reduce threats and/or mitigate impairment to family privacy, reputation, safety, digital, financial and physical assets.

Best Practices Highlights

- Cyber security best practices include tips on protecting family privacy, reputation and digital assets; and securing wireless networks, email, passwords and device security.
- Best practices for social media security calls for aligning online behavior with the family's mission, vision, values and ethics. Included are tips to avoid reputational damage, cyber crime, cyber bullying and personal liability.
- Travel security best practices include security planning prior to departure, ensuring that proper protocols are in place for the destination, knowing what to do during travel and if an emergency arises.
- Physical security best practices begin with vulnerability assessments of personal and business locations; and offers measures to protect family and their physical assets.

The Appendix contains security and insurance resources for cyber, travel, personal and identity security. An identity theft recovery plan checklist with resources, sample digital estate planning language and related studies and articles are also included.

CODE OF CONDUCT FRAMEWORK

1. **Objectives**
    a. Protect company and personal assets - physical, digital and reputational.
    b. Set clear expectations on acceptable behavior on and offline.
    c. Ensure stakeholder engagement and adoption.
    d. Enable online activity in a manner consistent with mission, vision and values.

2. **Approach/Process**
    a. Identify and engage key stakeholders from all generations to identify areas of concern and acceptable behaviors.
    b. Where appropriate, coordinate with operating business's policies and protocol.
    c. Consider how you will measure success.
    d. Incent younger generations to participate and comply.
    e. Review best practices for cyber, social media, travel and physical security.
    f. Educate, share and secure feedback from all family members.
    g. Work collaboratively with business enterprise risk managers (if applicable) to ensure that blended personal and business risks are identified and addressed.
    h. Finalize Code of Conduct, secure signatures and provide copies to family members.
    i. Review, report findings and update annually.

3. **Suggested Code of Conduct Structure**
    a. Family Mission, Vision and Shared Values
    b. Family Code of Ethics and Conduct
    c. Cyber Security Code of Conduct
    d. Social Media Code of Conduct
    e. Travel and Physical Security Protocols
    f. Contacts and Resources

Begin with an Overall Risk Assessment

Family office security experts advise that adopting a risk-based approach to security requires:

- Conducting a professional risk assessment based on validated information.
- Providing an accurate and truthful analysis.
- Ongoing assessment activity involving the right people, technology and processes.
- Earning the family's trust and support.

CYBER SECURITY BEST PRACTICES

I. Protect Family Privacy

a. Do not post personally identifiable information (PII).
b. Identify theft monitoring services to monitor:
   i. Credit reporting agencies.
   ii. Financial accounts activity including purchases, loans, withdrawals, etc.
   iii. Fraudulent activity and crimes.
   iv. Fraudulent healthcare services.
   v. Restore identity if stolen
c. Use cyber security experts to:
   i. Conduct annual online vulnerability assessment.
   ii. Remove PII and fake information from databases.
   iii. Provide reputational risk weekly report.
d. Consult with legal and security experts if drone surveillance is suspected.
e. Provide a "work only" device to staff with access to family information, not allowing them to intermingle family information with their personal information. Train staff to use work device for work only purposes.
f. Protect the privacy and physical safety of children using smart toys that have microphones, cameras, and GPS sensors. Before purchasing a connected toy, examine the firm's user agreement disclosures and privacy practices, and understand where data is sent and stored. Parental consent, asking knowledge-based authentication questions and using facial recognition to get a match with a verified photo ID are Federal Trade Commission requirements for children under 13.

II. Protect Digital Assets

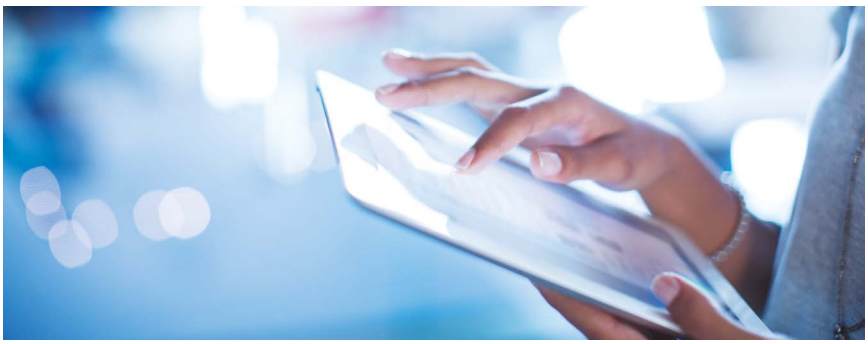
a. Back up digitally stored content: pictures, files, data, etc. on 1-2 local devices in addition to cloud storage.
b. Consult a cyber security expert if ransom is requested to unlock encrypted data.
c. Protect company social media sites by reporting inappropriate behavior to sites and pre-designated company resources.
d. Plan for online accounts (social media, email, storage, domains) at death or incapacitation. Some providers allow the account owner to grant account access permission to others. Other providers will only deactivate, remove or memorialize an account. Due to privacy reasons, it is unlikely that any provider will provide the account owners login information. See Resource list for links.
e. Do not store or send confidential information electronically unless encrypted.
f. Avoid storing confidential or proprietary information on USB flash or thumb drives, as they are easily lost/breached. If you must, use an encrypted device.
g. Avoid accessing online accounts from public computers and/or non-secure devices. If you must, do not save information, logout and close browser.
h. Utilize two-factor authentication for changing online accounts.

III. Protect Family Reputation

a. Do not share any information digitally that you do not want made public, even if with a friend, as it can be forwarded and or compromised.
b. Recognize that personal and business online activities often overlap and create risk to the family enterprise.
c. Monitor and report on online activity weekly.
d. Create a crisis management plan that includes triggers, notification, public relations response and database removal.
e. If you suspect that PII of employees, customers, etc. has been hacked, consult an attorney to secure forensic specialists to investigate. Attorney/client privilege may preserve confidentiality of findings, as files are non-discoverable.

IV. Secure Wireless Networks

a. Do not use open Wi-Fi networks. Use VPN if unavoidable. Delete network from device afterward to ensure automatic connection does not occur.
b. Avoid public Wi-Fi without VPN, even if password protected (i.e.: hotels).
c. Utilize cell or portable wireless router when traveling.
d. Secure home wireless routers:
   i. With unique passwords



ii. Dual band wireless router
    1. Use one band for mobile devices and visitors. These devices are more susceptible and threaten other devices on the same network band.
    2. Use one band for smart home devices (entertainment and security systems lighting and temperature controls, etc.) and computers.

V. Secure Email

a. Avoid free email accounts (Gmail, Yahoo, etc.) for communicating family business, financial and personal information. Use company or personal domain.
b. Do not download files or click on links from unfamiliar sources or unexpected receipt even if from a known source. Copy and paste URL in browser instead.
c. Do not respond to emails requesting PII and financial information.
d. Set email filter to not download images automatically.
e. Do not use "unsubscribe" link in emails from a source that you do not have a relationship. Mark sender as "Junk" in email filter.

VI. Ensure Device Security

a. Secure all devices with strong unique passwords. For staff "work only" devices, choose a password known only by the family employer and staff member.
b. Install tracking software on all mobile devices.
c. Keep mobile devices physically secure. Do not leave device on a table in public or a hotel room unless in a safe.
d. Do not download non-work related apps on work mobile devices.
e. Avoid plugging free/found USB flash/thumb drives in computer to minimize viruses, malware and breaches.
f. Secure cameras on devices to avoid eavesdropping/spying.
    i. Turn off or cover camera on computers when not in use.
    ii. Place camera face down on devices to obstruct view of spying attempts.
g. Select Internet connected smart home devices that have the following integrated security features to avoid unwanted access to device data, accounts, cameras and transmission by third party. These include secure boot, secure key storage, encryption and multifactor authentication. Change default ID's and passwords, and institute strong passwords.
h. Avoid unwanted access to smart speakers (Amazon Echo, Google Home, Apple HomePod):
    i. Turn off when not in use
    ii. Place out of view of windows, doors, etc.
    iii. Consider those with voice recognition capabilities.
i. Keep operating systems, anti-virus software and applications updated by enabling automatic updates.
j. Protect gaming devices by installing games from official stores, never from unsolicited offers.
k. Avoid communication to external sources on smart home devices.
l. Enable full disk encryption on devices in the event they are lost.
m. Enable using wireless keyboards/mouse when travelling, as there is no authentication and connected devices can be easily breached.
n. Register numbers with "Do Not Call" Registry. https://www.donotcall.gov/register/reg.aspx
o. Consider purchasing cyber insurance products that provide coverage for data restoration, cyber extortion, crisis and reputation management, and cyber bullying expenses. Many also provide access to restoration services and security specialists.

VII. Secure Passwords

a. Secure all devices with strong unique passwords.
b. Secure all online accounts (streaming services, email, social media, banking, etc.) with unique passwords.
c. Do not store passwords on devices or public clouds.
d. Utilize encrypted password managers to store passwords.
e. Use browsers suggested passwords and/or stored passwords only on password secure devices.

VIII. Implement Cyber Security Controls

a. Conduct regular risk assessment of family members, household staff, and family office staff across functions.
b. Conduct regular risk assessment of external vendors (see References for 40 Question checklist).
c. Implement cyber security policy and protocols internally and externally.
d. Hire third party auditor to conduct annual cyber security audit to test compliance.
e. Revise controls as warranted.

SOCIAL MEDIA SECURITY BEST PRACTICES

I. Behave consistent with family mission, vision and values.

II. Follow Family Code of Ethics and Conduct.

III. Observe legal and regulatory requirements.

IV. Be transparent about who you are.

V. Do not disclose personal and financial information about the family.

VI. Be courteous and respectful of others.

VII. Report instances of cyber bullying to sites where they occur and family designated resources.

VIII. Avoid controversial topics and negative reviews of products and businesses to minimize targeted lawsuits.

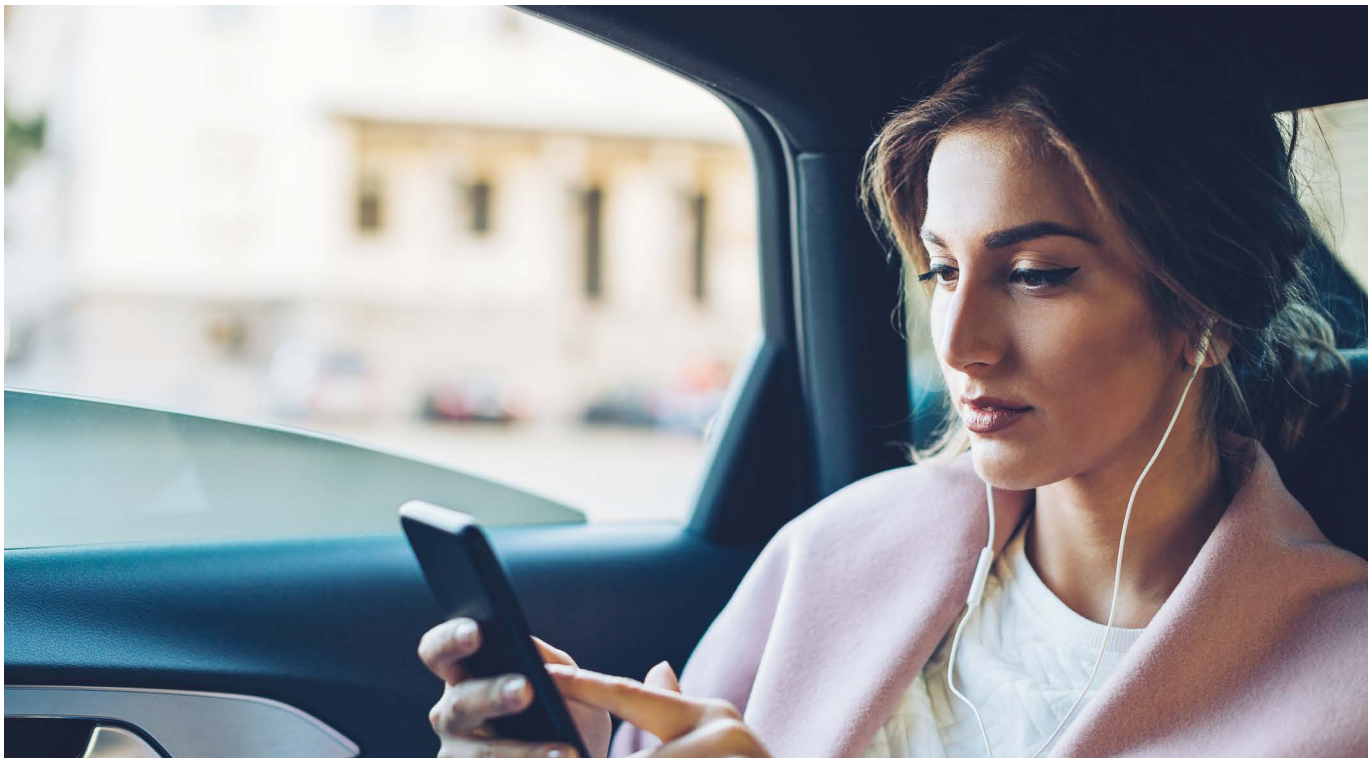
IX. Avoid letting the public know where you are or where you are going. Do not post your current location or plans, and hold off on posting pictures until you return home.

X. Select online "friends" that you know and trust. Be aware that unusual requests could be from a stolen social media identity.

XI. Use privacy settings to limit viewing outside of friends and /or network.

XII. Do not share social media site passwords and update frequently.

XIII. Verify that your liability insurance policy will respond to allegations of cyber bullying, personal injury and cyber crime. Some contain exclusions and limitations.



TRAVEL SECURITY BEST PRACTICES

I. Prior to departure:

a. Work with a security expert to develop journey management plan.
b. Evaluate travel protocols, transportation methods and contingencies:
   i. Learn local culture and risks associated with destination.
   ii. Vet hotel and drivers before booking reservations.
c. Check U.S. State Department's Travel Alerts and Warnings.
   i. Avoid travelling to locations under warning
   ii. Understand alerts: plan to minimize danger
   iii. Enroll in Smart Traveler Enrollment Program (STEP).
   iv. Consult with security specialists for further protocols.
d. Have an emergency response plan for medical care, including facility locations, evacuation, communication and access to professional guidance during crisis.
e. When renting a private residence at home or abroad, consider the hotel emergency services that will be lacking to guide emergency knowledge of evacuation routes, location of medical facilities and access to news, cell, GPS, etc.

II. During travel:

a. Use GPS tracking to be notified of alerts in close proximity.
b. Have situational awareness at all times.
c. Always use licensed transportation.
d. Be aware of local customs and laws.
e. Know and employ hotel best practices.
f. Use an abundance of caution when conducting any activity online.
g. Ease off social media and avoid posts related to where you are or aren't.

III. Purchase insurance to defray unforeseen costs and provide valuable assistance, such as:

a. Trip cancellation and interruption.
b. Emergency evacuation and repatriation of remains.
c. Travel medical assistance and pre-existing condition exclusion.
d. Worldwide travel assistance, concierge and emergency services.
e. Identity theft and roadside assistance.
f. Kidnap, ransom and extortion.
g. Political risk.

PHYSICAL SECURITY BEST PRACTICES

I. Conduct vulnerability assessment to identify areas of concern.

II. Balance security measures with desired level of intrusion.

III. Utilize geo-fencing to automatically secure property when leaving, limit unauthorized access and/or track when entering or exiting home/ business perimeter.

IV. Maintain records, monitor and manage specifics threats and threat scenarios.

V. Consider use of personal bodyguards ongoing or in high profile/high risk situations.

VI. Maintain situational awareness offline and online.

VII. Ensure home and office security systems are properly maintained and tested.

VIII. Perform routine physical security assessments.

IX. Regularly vet "inner circle" employees, advisors, and vendors.

X. Maintain a family emergency plan, including how to obtain professional crisis guidance.

XI. Consult with security experts if threats and/or ransom requests received.

XII. When purchasing insurance to protect homes, autos, valuables and family, utilize insurers and brokers who:
   a. Have expertise in family wealth lifestyles and passions.
   b. Are consultative, pro-active and responsive to client preferences.
   c. Tailor coverage and services to the unique needs of each family.
   d. Provide risk management and catastrophe planning/mitigation services:
      i. Wildfire / hurricane / flood prevention and response.
      ii. Consultation during build and re-build to mitigate future risk.
      iii. Private staff and blended personal/commercial exposures.
      iv. Family security and safety.

XIII. Consider Kidnap, Ransom and Extortion insurance coverage for all family members. Check with operating business to see if coverage is in place and extends to non-business family members.

REFERENCES

BITSIGHT - 40 Questions You Should Have in Your Vendor Security Assessment (November 04, 2015)

The Family Wealth Alliance Webinar: Results of Second Annual Survey, February 22, 2017.

Illinois Institute of Technology Code of the Family Ethics (2010)

Coca Cola Company Online Social Media Principles

www.dell.com/learn/us/en/uscorp1/corp-comm/social-media-policy?c=us&l=en&s=corp

Cyber Security Institute Code of Ethics & Conduct

Embedded Systems Engineering – Protecting Smart Home Devices from Security Breaches; Hal Kurkowski and Scott Jones, Maxim Integrated Design

Time (July 16, 2013)- How to Access a Deceased Loved One's Online Accounts; Doug Aamoth

FBI Public Service Announcement (July 17, 2017) CONSUMER NOTICE: INTERNET-CONNECTED TOYS COULD PRESENT PRIVACY AND CONTACT CONCERNS FOR CHILDREN

FBI Public Service Announcement (May 4, 2017) BUSINESS E-MAIL COMPROMISE

E-MAIL ACCOUNT COMPROMISE - THE 5 BILLION DOLLAR SCAM

PRMA Summit: Staying Safe – Physical, Cyber and Travel Security in a Rapidly Changing World; Jordan Arnold & Joseph Lawlor – K2 Intelligence.

PRMA Enlightenment Series (September 2016)- Personal Cyber Perils Explained and the Emerging Insurance Response; Norm Thoms and Timothy J. Zeilman- The Hartford Steam Boiler Inspection and Insurance Co.

Is the Malware Tidal Wave Ready To Sweep Away Your Staff's Mobile Devices? (July 14, 2017); The McCalmon Group, Inc.

Southeastern Family Office Forum Workshop: Hidden Security Risks and Solutions for Families and Family Enterprises (September 25, 2017)

Lisa Lindsay, Executive Director of the Private Risk Management Association

Mariann Mihailidis, Managing Director of the Family Office Exchange

Kristin Martin, Supervisor of Family Office, Love's Travel Stops & Country Stores

APPENDIX

CYBER AND TRAVEL SECURITY AND INSURANCE RESOURCES

Cyber Security

Services

- K2 Intelligence Cyber HouseCall®
- Rubica
- LookingGlass Cyber Solutions, Inc.

Cyber Risk Insurance

Business & Enterprise

- Corporate Data Risk, Business Interruption, Cyber Extortion and More
- Bodily Injury, Property Damage, Business Interruption and Product Liability
- Personal Identity Coverage for Customers & Members

Individual & Families

- Personal & Family Cyber

Travel Security

- US State Department Travel Alerts & Warnings
- Smart Traveler Enrollment Program (STEP)
- Safe Passage Travel Security
- Solace Global Risk View

Travel Insurance

Business & Enterprise

- Trip interruption, Trip Delay, Lost Luggage, Medical Expenses, Business Assistant Services & More

Family Travel

- Trip interruption, Medical Expense, Emergency Travel Services & More

Medical

- World Clinic

PERSONAL SECURITY AND INSURANCE RESOURCES

Personal & Family Security

- K2 Intelligence Private Client Services
  - Inner Circle Due Diligence
  - Physical Security
  - Personal Threat Hotline
- Solace Global Family & Executive Protection
- G4S Integrated Security Solutions

Personal Insurance

- AIG Private Client Group Insurance Services
- Loss Prevention Services
  - Wildfire Protection Unit
  - Hurricane Protection Unit
  - Preserving Private Collections
  - Personal & Home Security
  - Proactive Loss Prevention Strategies
  - Evacuation 101: What to know if you are forced to go
  - Protecting Second Homes
  - What to Consider When Choosing a Caretaker

IDENTITY SECURITY AND INSURANCE RESOURCES

Identity Theft

- Prevention Tips & Free Resources
- Reporting
  - Federal Trade Commission
    - Report or call 1-877-438-4338
    - Recovery Plan Steps
  - FBI
  - Experian or call 1-888-397-3742
  - Trans Union or call 1-800-680-7289
  - Equifax or call 1-888-766-0008
- Free Credit Report or call 1- 877-322-8228
- Monitoring & Recovery Services
  - IdentityForce
  - CyberScout

Identity Theft Insurance

- Identity Theft & Online Fraud

IDENTITY THEFT RECOVERY PLAN CHECKLIST & RESOURCES

For a detailed checklist see www.identitytheft.gov

What To Do Right Away

- Call the companies where you know fraud occurred
- Place a fraud alert and get your credit reports
  - Experian www.Experian.com/fraudalert or call 1-888-397-3742
  - Trans Union www.TransUnion.com/fraud or call 1-800-680-7289
  - Equifax www.Equifax.com/CreditReportAssistance or call 1-888-766-0008
  - Identity Theft Letter to Credit Bureau
  - Secure Free Credit Report or call 1- 877-322-8228
- Report identity theft to the Federal Trade Commission (FTC)
- You may choose to file a report with your local police department
  - FTC Memo to Law Enforcement

What To Do Next

- Close new accounts opened in your name
- Remove bogus charges from your account
- Correct your credit report
  - Identity Theft Letter to a Credit Bureau
- Consider adding an extended fraud alert or credit freeze
  - State Laws

Other Possible Steps

- Report a misused Social Security Number
  - Apply for new card
  - Check for activity
  - Contact local office
- Stop debt collectors from trying to collect debts you don't owe
  - Identity Theft Letter to Debt Collector
- Replace government issued IDs
  - Social Security Card/Number
  - Passports – State Department call 1-877-487-2778
  - Drivers License - State Departments of Motor Vehicles
- Clear your name of criminal charges
  - State Attorney General Office

Steps for Certain Accounts

- Utilities
  - Ask service provider to close account
  - For additional help, contact the State Public Utilities Commission
- Phones
  - National Consumer Telecom and Utilities Exchange for NCTUE Data Report or call 1-866-349-5185
  - File a complaint with the Federal Communications Commission at 1-888-225-5322 or TTY 1-888-835-5322
- Government Benefits
  - Local Government Benefits
  - Social Security Benefits or call 1-800-269-0271
- Checking Accounts
  - Bogus Account Opened - Free ChexSystems Report or call 1-800-428-9623
  - Fraudulent Checks Against Account
    - Telecheck 1-800-710-9898
    - Certegy 1-800-437-5120
- Student Loans
  - Request school or program to close account
  - Federal Student Loans – Fraud Hotline call 1-800-647-8733
- Apartment or House Rentals
  - Request tenant history report and request correction
- Investment Accounts
  - Contact broker or account manager
- Bankruptcy filed in you name
  - Write to regional trustee
  - Consider hiring an attorney through ABA or legal services provider

Special Forms of Identity Theft

- Tax Identity Theft
  - Complete IRS Identity Theft Affidavit
  - Place fraud alert with one credit bureau (they must report to others)
    - TransUnion or call 1-800-680-7289
    - Experian or call 1-888-397-3742
    - Equifax or call 1-888-766-0008
  - Secure Free Credit Report or call 1- 877-322-8228
- Child Identity Theft
  - Send letter with Minor Status Declaration
  - Request manual search of report by credit bureaus and remove account(s)
    - TransUnion
    - Experian
    - Equifax
  - Request credit bureaus freeze social security number
    - TransUnion
    - Experian
    - Equifax
- Medical Identity Theft
  - Request medical records from all doctors and all providers
  - Check state public health privacy laws
  - If not provided within 30 days, file complaint
  - Medical billing errors on credit report, follow 1-4 in What to do Next

DIGITAL ESTATE PLANNING – HOW TO ACCESS DECEDENTS' ACCOUNTS

Facebook	**Google**	**Yahoo**	**Instagram**	**Apple**	**Dreamhost**
LinkedIn	**Microsoft**	**Twitter**	**Snapchat**	**GoDaddy**	

DIGITAL ESTATE PLANNING

Sample Language for your Will or Revocable Trust regarding Digital Assets
Power of Trustee or Executor

To access, use, and control settlor's digital devices, including, but not limited to, desktop computers, laptop computers, tablets, peripherals, digital data storage devices, mobile telephones, smartphones, and any similar digital device which currently exists or may exist as technology develops for the purpose of accessing, modifying, deleting, controlling, or transferring settlor's digital data and digital assets. Trustees shall have the power to access, modify, delete, control, and transfer settlor's digital data and digital assets, including, but not limited to, the following: settlor's e-mails received, e-mail accounts, digital music, digital photographs, digital videos, software licenses, social network accounts, file sharing accounts, financial accounts, banking accounts, domain registrations, DNS service accounts, web hosting accounts, tax preparation service accounts, online stores, affiliate programs, other online accounts, and similar digital items which currently exist or may exist as technology develops. Trustees shall have the power to obtain, access, modify, delete, and control settlor's usernames, passwords and other electronic credentials associated with settlor's digital devices and digital assets described above.

RELATED STUDIES AND ARTICLES

- Internet of Things (IoT) Infographic
- The Internet of Things: Evolution or Revolution?
- IoT Case Studies: Companies Leading the Connected Economy
- The Date Sharing Economy: Quantifying Tradeoffs that Power New Business Models
- Internet of Things (IoT) Risk Manager Checklist
- Creating a Digital Estate Plan
- How to Close Online Accounts and Services When Someone Dies

AIG Private Client Group is proud to work with a select group of the finest independent insurance agents and brokers. To learn more, please visit www.aig.com/pcg

American International Group, Inc. (AIG) is a leading global insurance organization. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig. These references with additional information about AIG have been provided as a convenience, and the information contained on such websites is not incorporated by reference into this press release.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.

© 2018 American International Group, Inc. All rights reserved.

04/18 6285T