MERRILL
A BANK OF AMERICA COMPANY

CYBERSECURITY

Modern Security for the Family Office

Protecting a family's resources and privacy requires a platform that combines cutting edge technology, rigorous standards and customized client services.

FAMILY RESOURCES CAN PROVIDE COMFORT, security and opportunity to children and future generations and help promote a family's values through philanthropy. In the digital age, an increasing share of family resources are stored as information in virtual accounts. But protecting data is just as challenging as securing hard assets. As technology has become more sophisticated, the threats to vital personal information have grown accordingly. More than ever, protecting extended families against unseen threats requires rigorous digital security and protocols.

A family office that coordinates protection and access to resources can deliver the dual benefit of security and simplification to the families it serves. It can provide the structures, and foster the unity, that help families achieve various goals with a high level of service, integrity and confidentiality.

Family office professionals can help attend to your loved ones' financial needs, facilitate family governance, support multiple households in an efficient way, pursue your philanthropic vision and protect your legacy and succession plans. Above all, a family office should deploy the most robust defenses to facilitate access and control of your resources and maintain your confidence in their effectiveness.

To enable that confidence, family offices should employ a set of services and defenses to meet each family's unique needs, which usually will include data aggregation, bill payment, accounting, liquidity management and electronic document vaulting. Collectively, these services are known as the "family office platform."

Growing cybersecurity threats warrant a significant investment in digital security and family office operations.

A platform should combine digital security controls and meticulously designed processes that help facilitate safe transactions and protect and organize critical data. To achieve service integrity and robust security, the platform should be adaptable, flexible and supported by innovative, strategic thinking. At Merrill, we believe that the best solutions leverage family office and information security expertise, innovative processes and best-in-class technology partners. These elements can create a distinctive, secure and efficient platform specifically designed to meet the needs of every client, while facilitating safe transactions and organizing critical data.

Whether high-net-worth families want to work with an institutional partner or create an independent family office, we encourage them to meet with our experts and learn more about the optimal security features they should depend on to protect their assets and legacies.

A PRIVATE ENVIRONMENT FOR SERVICES AND CLIENT INFORMATION

High-net-worth individuals and families with extensive investments in a wide range of asset classes, revenue and payment streams, and multiple professional advisors occupy complex ecosystems. As cybersecurity events continue to make headlines and criminals concentrate their efforts on enterprises and wealthy individuals, it's more important than ever to protect every surface of these families' operations and critical information with the best security controls available.

The need to simplify networks and make clients' assets work for them compounds the family office challenge. The wrong solution can lead to an overly complex and restrictive support model that hampers clients, heightens security risks or both.

An effective solution to this challenge involves designing and building a centralized digital platform, maintained as a single, integrated technology to specifically serve the needs of affluent families. Platform configuration should allow regimented access to the family's support team and interface seamlessly with other, essential data platforms

of the family's investment management and other critical advisors. The technology provider should commit to upholding the same security standards.

The platform should also support the most critical family office functions: data aggregation, accounting, bill pay, liquidity management, information storage and electronic vaulting. Any links between a client's domain names, vendors and internal communications should include automatic encryption, which protects the information channels flowing into and out of the platform by default.

Service for every client begins with peace of mind, however protecting family office clients with the most complex accumulation of assets and interests requires extra steps. An internal board of security experts should perform ongoing review and approval of the architecture and security controls of an institutional family office platform to establish that it operates on the most rigorous security standard. Internal and third-party vendors should conduct regular assessments to ensure defenses remain robust and current. In light of the changing cybersecurity environment and development of new tools, the platform's technology experts should make updates to address the emerging threat landscape.

The most secure office will operate off a standalone digital platform specifically designed to meet the needs of high-net-worth families.

Families should have their information flow seamlessly from multiple investment providers and advisors into the platform, resulting in a single, consolidated balance sheet. Any family office should be agnostic in terms of assets and custodians. This supports assembly and storage of information from accounts held with any other institution or documenting any asset in protected layers of the platform, including the electronic vault.

ACCESS CONTROLS THAT WORK FOR AND PROTECT CLIENTS

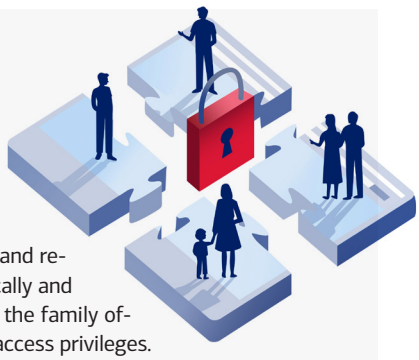
Security is not simply a function of guarding all channels that flow into and out of the family office platform. Clients also need to know that only family office professionals or other trusted advisors have access to see their data. The platform should enable all family office associates to use single sign-on protocols to access the platform, which streamlines and internalizes password security. These controls should also ensure automatic privilege revocation as soon as any associate leaves the team.

Families need to know that their data is secure and only available to those who need to see it, and that their approvals are reinforced by strict access review management controls.

A decision to grant platform access to trusted advisors outside the family should require, at a minimum, multifactor authentication access controls. Many families may prefer additional controls that enable access only to specific layers of the platform to further secure information privacy. Since multiple third parties (such as lawyers, accountants and advisors) may need access only to certain documents or files, their sign-on credentials should limit their view

Essential security features of the family office

The family office platform should provide seamless functionality while maintaining strong security features and protocols. These strategies and technologies can help establish the right balance of control and simplified operations:



Security review board assessment. Families should rely upon technical expertise to validate the effectiveness of the platform's security tools and vendor agreements.

Platform privacy and backup. The family's platform should be dedicated solely to supporting the needs of family office clients. All client data and electric vault contents should be stored and backed up in data centers controlled by a single technology provider.

Transport Level Security (TLS). All communications with the family and technology partners should employ encryption through TLS controls, which reduces the possibility of human error and potential breaches.

Robust access review management. The family should determine platform access for internal officers and third parties. Single sign-on (SSO) technology, paired with multifactor authentication, should verify all log-in identities and revoke access privileges automatically and immediately when officers leave the family office or clients revoke third-party access privileges.

Data access controls. The platform should allow clients to approve third-party access only to the account or portfolio details they need, without any exposure or compromise of other data.

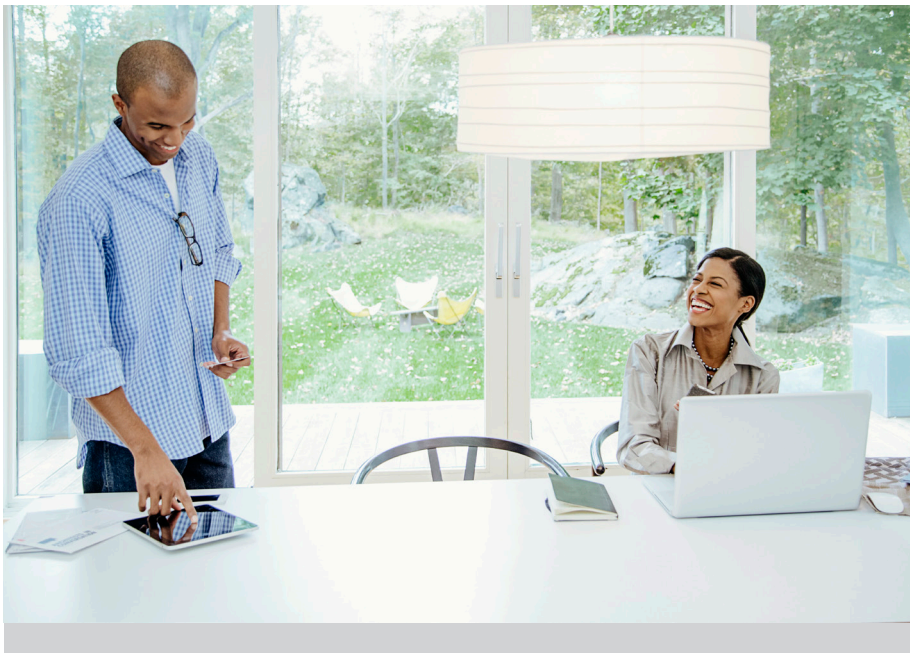
Best-in-class technological support. Whether institutional or independent, family offices should engage technology providers who secure networks and operations for global enterprises.

Annual risk assessments and scans. The best defense is never complacent. The family office platform should be regularly means-tested and reviewed by internal technicians and leading third-party security experts.

to only the information a client approves. This technological design provides access as broad or narrow as each client requires without unnecessary or cumbersome controls.

PAYMENT VERIFICATIONS LEVERAGING AUTOMATION AND AUDITABLE, MULTI-LAYERED APPROVALS

Facilitating bill payment for clients with many obligations highlights the challenging balance between platform security, functionality and simplified client processes.



While every family requires security, many clients prefer to handle only the largest or most anomalous transactions themselves. Achieving the right balance for every client depends on preset payment thresholds, strict payee authorization protocols, advanced fraud detection software and compliance with high fiduciary standards.

Protections should begin with the family authorizing the office to pay bills to certain payees in amounts below set thresholds. Fraud oversight tools should inspect each automated payment, however routine, to verify transaction amounts, identification numbers and recipients. We recommend that any family office maintain this oversight through regular testing and monitoring.

Approving most payments above the threshold through an auditable, automated dual-authentication procedure leaves the client to directly authorize only the largest and least classifiable payments. But in every case, creating and maintaining a new payee profile should happen within a multi-tiered review process that mitigates risk without undue involvement from the client.

The family office should simplify operations through strict payee authorization protocols, preset payment thresholds and compliance with high fiduciary standards.

Since vendors often utilize their own digital and cloud technologies that may present distinct cybersecurity risks, the platform's technology controls should include additional oversight.

A SOLUTION BASED ON INTUITIVE PROCESSES AND THE BEST TOOLS

High-net-worth families have many choices for managing their wealth and operations. With so much to protect, they don't have to settle for anything less than leading technology and services that make complex operations transparent and manageable.

Key takeaways:

- Information security should serve as the foundation to all family offices, regardless of insourced or outsourced technology, with the commitment to regularly review and update the platform's security.
- Any family office should operate off a distinct digital platform specifically dedicated to supporting the needs of high-net-worth families and employing best-in-class providers to build and sustain a robust and secure technological architecture.
- Every family office should have current and adaptable security. Technology partners should embrace the highest industry security standards and regularly assess their defenses.
- Payment and transaction automation will vary depending on each family's needs. The platform should adapt to each family's risk tolerance and operational requirements.
- Reach out to your personal wealth advisor for more information concerning family office services and security controls.

At Merrill, we believe any family office should combine the power of institutional technology with a deep understanding of the family's needs and expectations. Bringing all family office functionality onto a discrete platform, subject to continual reassessment and improvement, creates an environment that manages data storage, authorizations and payments with transparency, ease and confidence.While this requires significant, ongoing technology innovations and cutting-edge strategizing, a robust platform can meet the challenge of balancing functionality and security and preserve opportunity for current and future generations.

IMPORTANT INFORMATION

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

Family Office Services are offered through MLPF&S. In connection with its Family Office Services, Merrill is not acting in the capacity as a broker-dealer, nor as a registered investment adviser. Accordingly, through its Family Office Services, Merrill is not offering, and its clients are not paying for, advice with respect to securities, the purchase or sale of securities or the valuation thereof, nor do Family Office Services encompass financial planning, discretionary account management or any other securities-related accounts, products or services.

Merrill Lynch, Pierce, Fenner & Smith Incorporated (also referred to as "MLPF&S" or "Merrill") makes available certain investment products sponsored, managed, distributed or provided by companies that are affiliates of Bank of America Corporation ("BofA Corp."). MLPF&S is a registered broker-dealer, registered investment adviser, Member SIPC and a wholly owned subsidiary of BofA Corp.

Trust, fiduciary, and investment management services are provided by Bank of America N.A., Member FDIC, and wholly owned subsidiary of Bank of America Corporation ("BofA Corp."), and its agents. Bank of America Private Bank is a division of Bank of America, N.A. Banking products are provided by Bank of America, N.A., and affiliated banks, Members FDIC and wholly owned subsidiaries of BofA Corp.

Merrill Private Wealth Management is a division of MLPF&S that offers a broad array of personalized wealth management products and services. Both brokerage and investment advisory services (including financial planning) are offered by the Private Wealth Advisors through MLPF&S. The nature and degree of advice and assistance provided, the fees charged, and client rights and Merrill's obligations will differ among these services. Investments involve risk, including the possible loss of principal investment. The banking, credit and trust services sold by the Private Wealth Advisors are offered by licensed banks and trust companies, including Bank of America, N.A., Member FDIC and other affiliated banks.

Investment products:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value