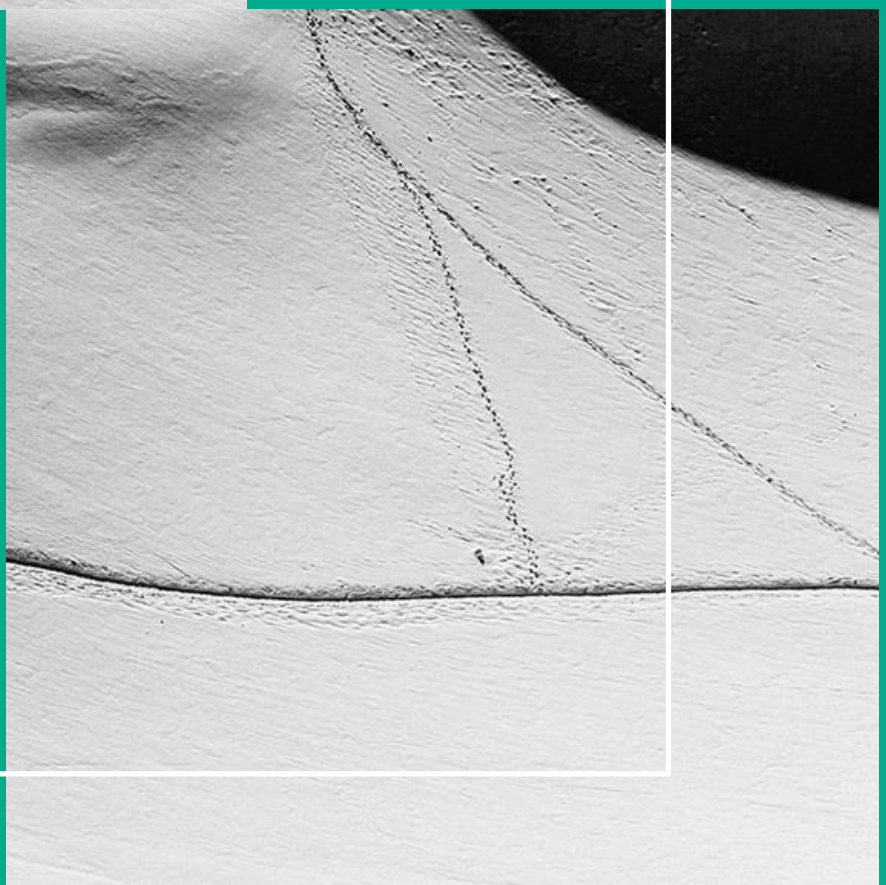
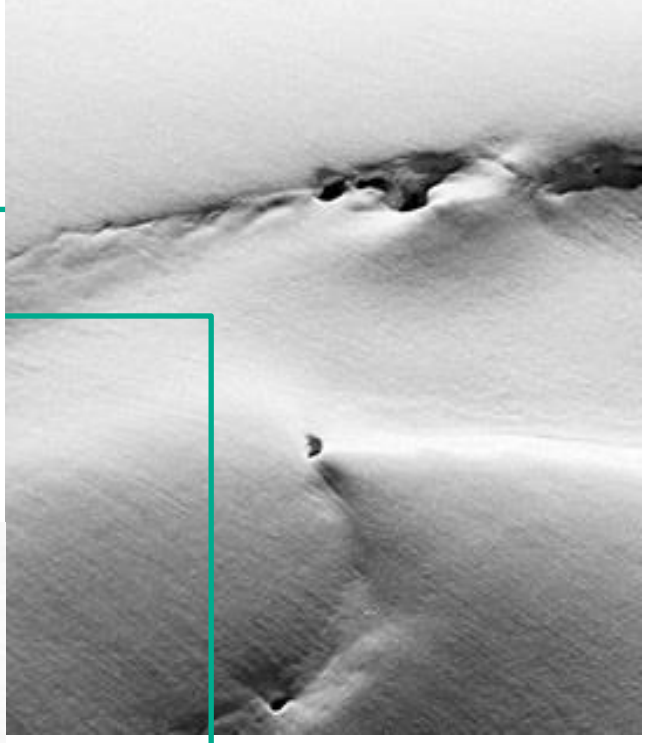
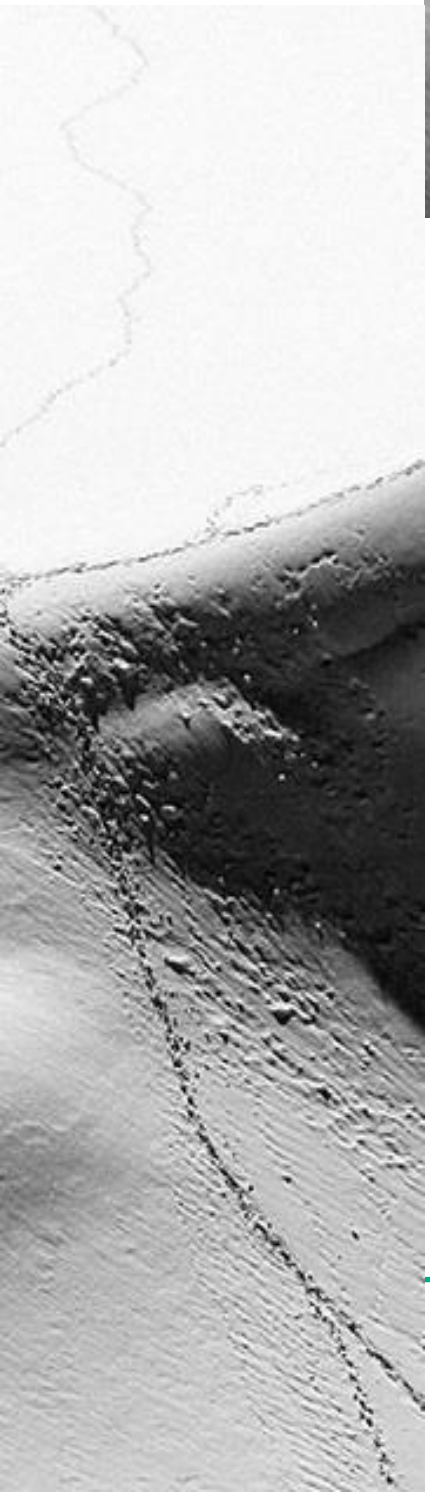
CAPCODIGITAL

DIGITAL RISK MANAGEMENT







DIGITAL RISK MANAGEMENT: HOW SECURE IS YOUR DIGITAL WEALTH OPERATING MODEL?

Capitalise on the next wave of digital opportunities in Wealth Management by implementing a truly enterprise-wide Digital Risk Management approach to secure the digital operating model and underpin client trust.

“ The momentum of digital change in Wealth moves forward at pace presenting Wealth Managers with a number of opportunities but equally exposing them to emerging data security risks. “

The digital wealth economy: an evolving landscape

The Wealth Management industry is undergoing an unprecedented wave of digital transformation. Wealth Managers are transforming their operating models and underlying infrastructure to be fit for purpose in a digital age. Coupled with changing client needs, the momentum of digital change in Wealth moves forward at pace presenting Wealth Managers with a number of opportunities but equally exposing them to emerging data security risks. The drivers include continuous advances in technology, competition from fintech startups eroding parts of the wealth value chain, the availability of big and thick data and the need to cost-optimise and drive straight-through processing (STP). Combined with the proliferation of social platforms, the changing regulatory landscape and the rise of new data security threats, you have a ‘perfect storm’ of challenges to traditional Wealth Management operating models.

In this context, Wealth Managers are pushing forward with their digital transformation programmes. Their goal is to offer clients engaging, data- and functionality-rich, secure multi-channel experiences that provide access to their wealth anytime, anywhere. In parallel, Wealth Managers have been equipping their Relationship Managers and Private Bankers with powerful digital solutions to further improve their productivity, regulatory compliance and quality of advice and service provision.

These digital improvements are not limited to the front office. Significant transformation is impacting the entire front-to-back operating model, with the objective of fully harnessing the revenue, cost and compliance benefits of digital. The digital wealth economy is now truly in full swing and transforming the competitive landscape forever. In this new landscape, Wealth Managers are being exposed more than ever to digital risks to client privacy and data security which are not fully understood and holistically addressed by current digital transformation programmes. A revised approach needs to be adopted to enable Wealth Managers to capitalise on the opportunities and mitigate the risks of the digital wealth economy.

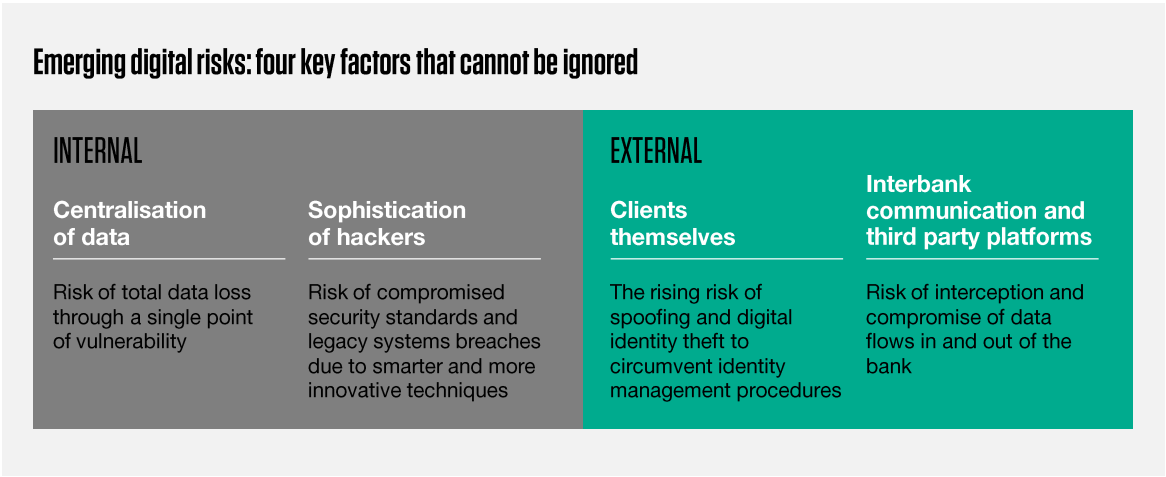
Emerging digital risks: four key factors that cannot be ignored

Over the last 20 years, Wealth Managers have had a tough and ongoing battle to maintain client privacy. In our age of regulatory transparency, the locked filing cabinet is long gone. Now, the locked database, front-end digital platform, execution management system and core banking engine - to name some of the key operational components - are also under threat. This is one of the realities – and the great risks - of our age of digital activism and cybercrime.

Unsurprisingly, cybercrime generates ever-growing concern in the C-suite. The breadth of its potential impact on Wealth Managers extends, but is not limited, to operations, brand reputation, client confidence, financial loss, IP loss and legal fines. Such impact can significantly inhibit, or even potentially ruin, a Wealth Manager. This is alarming yet hardly surprising, given that the entire business is founded on relationships, performance and trust. In the future, Capco perceives digital risks being exacerbated in four main ways: centralisation of data, sophistication of hackers, clients themselves, and interbank communication and third party platforms.

Centralisation of data. At one time, a breach in security would have exposed a limited amount of client information, relating perhaps to one single file, disc or office. Today, centralised storage of digital information means that just one point of vulnerability can result in total loss. The recent Panama Papers[1] leak, the largest leak of confidential information in history, provides a dramatic illustration. Admittedly, it originated from a legal firm, not a financial one. Surely banks, asset managers and private offices are more secure? The evidence to date suggests such hope is misplaced as the second issue, the sophistication of hackers, constantly evolves.

Sophistication of hackers. Rising global cybercrime shows that no industry is immune from this form of risk. The insurance company Lloyd's of London estimates the cost to businesses to be as much as $400 billion a year[2], which includes direct damage and post-incident disruption. According to TechSci Research, an IT market intelligence firm, the financial services industry is the sector with the highest levels of reported cybercrime incidents, followed by the telecommunications and defence sectors[3]. In February 2015, the largest global cybercrime ever uncovered in the financial services industry was reported in the media with stories that Russia-based hackers had



stolen up to 650 million pounds from banks in the U.S. Europe and the Middle East[4]. The hackers broke into banks' networks and spent months installing programmes and collecting data in order to withdraw money. Then in April 2016, Qatar National Bank reported a data hack. The theft of personal details, accounts and passwords exposed business leaders, royalty and prominent government officials.

> " Capco perceives digital risks being exacerbated in four main ways: centralisation of data, sophistication of hackers, clients themselves, and interbank and third party platforms. "

These are just two recent examples of cybercrime evolving to match and exploit digital proliferation within financial services. Wealth Managers are high profile targets for hackers, given that their clients possess significant financial wealth and social influence. Their risk potential is raised further by the myriad of legacy processes and systems that have been built over time across front, middle and back offices. Typically, these systems are not adequately resilient in the face of digital age demands and the growing sophistication and consequent threat posed by digital 'hacktivists'.

Clients themselves. Aside from any issues with the internal security standards implemented by Wealth Management providers, the third threat comes from the outside. And it derives from clients themselves. One of the most popular, and effective, forms of cybercrime is an update on old-fashioned 'spoofing'. Here, criminals exploit the huge amount of information clients and their families post on social media platforms. In February 2016, specialist security firm Kroll reported that funds had been stolen from family offices as the result of lax identity and security controls[5]. The lesson to be learned is this: pressure to deliver slick interfaces and delivery processes must be carefully balanced against the evolving digital security risk. Digital devices clients use to interact with their Wealth Manager must now be considered as centrally important within an overall infrastructure of security and privacy. Delivery of new and engaging client experiences across devices and wearables also means potential exposure to new channels of attack.

Interbank communication and third party platforms. The final issue is also external to the Wealth Manager. Interbank communication, again often provided through legacy systems, are slow to change. Their near-universal adoption and common standards mean inbuilt inertia. Yet they have been exposed as subject to attack. A recent incident on the SWIFT platform attacked the gateways of vulnerable banks or their partners. Millions of dollars were re-directed fraudulently, compromising a number of banks[6]. Wealth Managers also need to be mindful that risks extend into the usage of third party trading platforms, data exchanges with trading venues and brokerage platforms. Risks also extend through to the adoption of open APIs, the platform economy and blockchain.

The call to action: a multifaceted threat demands truly comprehensive Digital Risk Management

Yes, the climate is challenging. And yes, the evolving digital wealth operating model creates more potential exposure than ever before. But no, Wealth Managers are not powerless – far from it. A comprehensive **Digital Risk Management (DRM)** approach is at their disposal. It combines sound governance, process innovation and new security technologies with highly aware and well-equipped leadership. Its outcome is to ensure the digital relationship is more secure. And the more secure it is, the more trusted it will become.

In practical terms, Wealth Managers are progressing. They are moving forward with new forms of push authentication and biometrics that leverage advances in technology. Implemented correctly, these developments offer new routes to secure client information and communication. They are also tightening security standards and risk assessments when leveraging third party platforms. The challenge

remains however of holistically addressing the full range of security threats. Leaders in the Digital Wealth economy must now take an enterprise-wide view of their digital risks. They must adopt the DRM approach to effectively mitigate the ever-growing digital security threats to the client base and operating model. Robust Digital Risk Management processes and controls will underpin this approach. The clear and present imperative is to secure systems from attack. Optimised functionality will enable preventive alerting to intrusion or service denial attempts. And it will respond rapidly in the event of a breach.

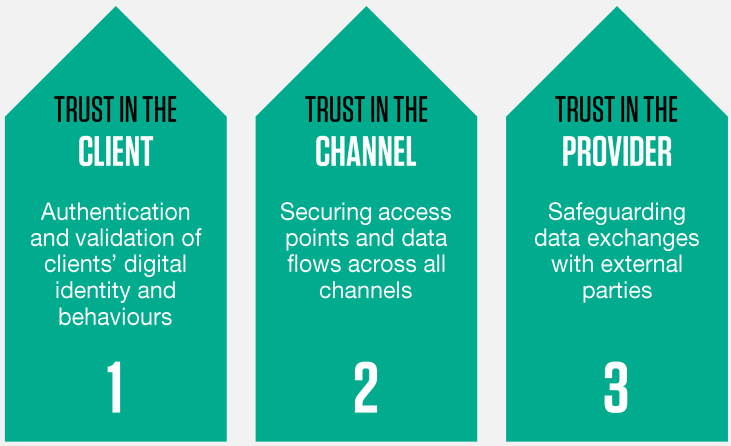
The end game for those who succeed in establishing a secure, digitally enabled operating model will be market leading entry into a new era of cutting-edge digital experiences. These will leverage strong relationships to deliver best-in-class wealth services. Crucially, they will also build and maintain trust in a digital age. In contrast, competitors who fail to innovatively address underlying digital threats will be exposed and potentially compromised. Nor is the discussion restricted to the client relationship. Wealth Managers will also come under greater scrutiny from regulators determined to ensure adequate measures, processes and standards are in place to mitigate digital risks.

Securing the digital wealth relationship: DRM and the three key axes of trust

From initial prospecting and onboarding through ongoing relationship management, the Wealth Manager needs to continuously mitigate digital risks. The reward is to build and maintain client trust, at each stage of the engagement lifecycle and through every data exchange and interaction. Securing trust by securing client sensitive data is quite simply critical for leaders in the Digital Wealth economy.

Capco categorises the digital security threats and risks that could compromise the relationship between Wealth Managers and clients into three key, interrelated axes of trust: the client, the channel and the provider.

Securing the digital wealth relationship: the three axes of trust



A truly comprehensive DRM approach ensures that all three key areas of trust are fully supported

Trust in the client requires a diligent approach to Knowing Your Customer (KYC), in order to identify both habitual and unexpected behaviours. This is a particular challenge with HNWIs. Wealth Managers must make sure that authentication is in place to know, with certainty, that any instructions really are coming from their clients. Managers and clients must also work together to prevent spoofing and other techniques that exploit material posted on social channels.

Trust in the channel grows in importance as Wealth Managers progressively adopt multi-channel servicing models. Greater access to position and performance information and new ways to interact and collaborate are empowering clients with a wealth of information and choice as relationships become increasingly digital. But, as clients come to rely on new channels, privacy, system accuracy, reliability and uptime become critical differentiating factors. Protection against denial of service and channel hacking becomes paramount in the new operating landscape. Clients expect absolutely watertight security, irrespective of their choice of channel, when accessing data related to their wealth and investments.

Trust in the provider must be (can only be) underpinned by the institution's relentless emphasis on maintaining client privacy. In turn, this emphasis must be actioned through a strong suite of security policies and technologies, extending right across the operating model and the underlying infrastructure. These will not be limited to securing client wealth and investment data on internal systems. They will take a holistic approach by securing broader data exchanges and flows, including third party platforms and any outsourced middle- and back-office operating models.

A truly comprehensive DRM approach ensures that all three key areas of trust are fully supported. The total trust relationship is managed effectively and holistically. Risks are recognised and mitigated before they result in any damage. Full client trust is maintained, even in the event of a compromise. Consequently, and in every sense, the relationship is secured. And those organisations clearly demonstrating their ability to support the trust relationship to their clients will place themselves at the forefront of the Digital Wealth economy.

> "Leaders in the Digital Wealth economy must now take an enterprise-wide view of their digital risks."

The way forward: securing the digital wealth operating model – operational considerations

Wealth Managers now have a clear agenda. They need to ensure their operating model is secure, fit for purpose and flexible in a fast-changing landscape. That's the principle. What are the practical operational considerations? To secure trust in the client, channels and provider, a truly comprehensive Digital Risk Management approach needs to be adopted as part of the next wave of digital transformation:

1. **Trust in the client** – Ensure digital authentication of clients, and closely manage client access, to minimise external visibility and mitigate spoofing. Leverage biometric technology to access and validate clients, accounts and transactions. Implement more advanced and secure identity and access management systems, integrated into a wider digitally-engaging client wealth management experience. Realise that the proliferation of self-directed and self-service investment capabilities - robo-advisors - means Wealth Managers simply cannot compromise client authentication and identity management.
2. **Trust in the channel** - Ensure delivery channels and the data exchanged through them are secured and monitored across all primary channels, including online, mobile, wearables, advisor (human and automated) and service support centre. Utilise, for example, encrypted wireless access, paired with authenticated devices, to connect to the digital services made available to clients to access and interact with their wealth and investment data. Wealth Managers will also need to secure data access and exchange via an RM-owned tablet as they cross borders advising their clients and disclosing wealth plans and investment strategies. This applies too when carrying out any real-time portfolio simulation, via a tablet that would require instantaneous two-way data exchanges with core banking platforms and risk engines.
3. **Trust in the provider** - Ensure the robust integrity of organisational infrastructure across internal platforms for both immediate Wealth-owned platforms and those shared with other parts of the bank. This applies also to third party systems for both on-premise and cloud-based applications, and any outsourced / offshored operating models that exchange business critical and client sensitive data. These must be secured to a level that mitigates threats, fully in line with the institution's risk appetite and overall business and data strategy. Ensure also that adequate digital risk management governance, roles and operating procedures are in place to detect, respond to and prevent digital risks. Ensure Digital Risk Management features prominently in an overarching strategy for a digital age, to confirm client and data security are factored into downstream change-the-bank initiatives and future digital operating models.

> "All our services are built on proven methodologies and frameworks, designed to prevent, detect and respond to digital threats and their impacts."

How Capco can help bring it all together

Capco can help Wealth Managers seeking either to initiate an effective approach to Digital Risk Management or to strengthen their current practice. We overcome the strategic and operational challenges inherent in specifying, implementing and securing the optimum digital operating model. We do this through assessment, planning and execution of a range of digital risk management services, for example upfront digital security diagnostics and capability assessments through to security target operating model & architecture design and implementation. These services are designed to be agile and to fully support business enablement. Their clear objective is to help Wealth Managers create and deliver a secure digital operating model, one that builds and maintains trusted client relationships in a digital age.

All our services are built on proven methodologies and frameworks, designed to prevent detect and respond to digital threats and their impacts. To support our clients, we exploit the deep expertise in cyber-security and digital capabilities combined with broad knowledge and 'hands-on' experience of digital transformation in Wealth Management. We are fully familiar with emerging Wealth Management operating models and trends. We also draw upon a rich ecosystem of carefully selected technical providers of cyber-security services. These providers fully complement, and are integrated within, our holistic Digital Risk Management services.

For more information on our Digital Risk Management services for Wealth Management, or our Digital services for Wealth Management, please contact a member of our expert team.

Capco team

- Christine Ciriani, Managing Partner, Global Head of Wealth & Asset Management
- Mark Stringer, Partner, UK Head of Wealth & Asset Management
- Nic Parmaksizian, Partner, Head of Capco Digital for EMEA & APAC
- Daniel Giannotti, Managing Principal, UK Wealth Management Lead
- Roy McNamara, Managing Principal, UK Digital Risk Management Lead
- Eoin Walshe, Consultant, UK Wealth Management

Capco Thought Leadership - Digital Trust Series

- Digital Trust
- Machine Learning & Cyber-Security

1. Panama Papers leak refers to a leak of 11.5 million files from the database of the world's fourth biggest offshore law firm, Mossack Fonseca, that detail financial and attorney–client information for more than 214,488 offshore entities. Source: Financial Times.
2. Source: forbes.com
3. Source: forbes.com
4. Source: bbc.co.uk
5. Source: Security Executive Council

6 Source: reuters.co.uk

AUTHORS

Daniel Giannotti
daniel.giannotti@capco.com

Roy McNamara
roy.mcnamara@capco.com

Eoin Walshe
eoin.walshe@capco.com

ABOUT CAPCO DIGITAL

Innovation begins with a vision. But bringing any vision to reality requires a lot more than imagination. It requires a complete understanding of what's possible and the know-how to make it happen. Regardless of the scope of our clients' visions for their future, at Capco Digital, we have the financial services experience and expertise necessary to bring those visions to life.

Where our clients bring a deep understanding of their own institutions, our global team of financial services and technology specialists brings a deep understanding of technological advancements, user-experience possibilities, and cultural savvy.

Not to mention, they're 100% dedicated to technology for financial services. We champion our clients' ideas with leading-edge design and technologies. We work with you rather than around you, collaborating to build solutions that will drive your institution, today and five years from now — solutions which businesses, consumers and investors can use every day.

Capco Digital. Collaboration to power finance. Ingenuity to push it forward.

WORLDWIDE OFFICES

Bangalore – Bratislava – Brussels – Chicago – Dallas – Dusseldorf – Edinburgh – Frankfurt – Geneva – Hong Kong – Houston – Kuala Lumpur – London – New York – Orlando – Paris – Singapore – Toronto – Vienna – Washington DC – Zurich

To learn more, contact us in the UK on +44 20 7426 1500, in Continental Europe on +49 69 97 60 9000, in North America on +1 212 284 8600, visit our website at CAPCO.COM, or follow us on Twitter @Capco

CAPCODIGITAL

CAPCO WORLDWIDE:

BANGALORE
BRATISLAVA
BRUSSELS
CHICAGO
DALLAS
DÜSSELDORF
EDINBURGH
FRANKFURT
GENEVA
HONG KONG
HOUSTON
KUALA LUMPUR
LONDON
NEW YORK
ORLANDO
PARIS
SINGAPORE
TORONTO
VIENNA
WASHINGTON D.C.
ZURICH