PROMONTORY Sightlines INFOCUS
promontory.com SEPTEMBER 18, 2013

BY ADAM SHAPIRO

The Way Forward for Digital Currencies

Adam Shapiro is a director at Promontory who focuses on helping clients strengthen compliance programs and address issues of regulatory concern.

Digital currencies have reached a critical — and delicate — moment in their evolution. U.S. regulators and law enforcement are increasingly focused on the potential use of digital currencies[1] to finance criminal activities, including terrorism.

Scrutiny in the U.S. affects not only domestic digital-currency firms, but also global digital-currency firms that have U.S. customers. Regulators outside of the U.S. have generally not yet indicated the same level of concern, but many are monitoring the digital-currency market and are likely to devote greater resources to its oversight if its growth continues.

The industry can take steps to ease regulators' concerns, but doing so will require major changes to current practices and technology. The formation of the Committee for the Establishment of the Digital Asset Transfer Authority, which will work with regulators and law enforcement worldwide to establish best practices and a self-regulatory organization for digital-currency firms, represents a positive first step toward these goals.[2]

The necessary changes will likely alienate some legitimate users who value the independence of digital currencies from the influence of national governments, but U.S. law enforcement and regulators expect the industry to make progress on these issues and have shown they will not hesitate to step in if the industry does not. Few firms like to upset customers, but the potential for increasingly severe enforcement actions — which are almost certain without further prompt action by the digital-currency industry — is an even greater threat to the industry's viability.

Two recent developments have raised the public profile of digital currencies and put them on regulators' radar. The first is the rapid growth in Bitcoin activity, including:

- Adoption of Bitcoin as a medium of exchange by a small, but growing, group of merchants, creating a nascent payments market for goods and services
- Use of Bitcoin as an alternative asset class, encouraged by a generally upward trend in the value of the currency. A bitcoin[3] traded at approximately $120 in early September, up from approximately $6 little more than a year ago

[1] This article is about decentralized, math-based digital currencies. Centralized digital currencies also require careful risk management, but the central issuer can more easily design a system that does not allow for anonymous users.
[2] In July 2013, a number of emerging payment, digital currency, and venture capital firms announced the creation of the Committee for the Establishment of the Digital Asset Transfer Authority. For more information, see http://www.datauthority.org.
[3] The concept of this digital currency, as well as the associated payments market, is Bitcoin; the currency unit is bitcoin.

Key Takeaways

- Digital currencies have great potential to improve the financial system by reducing payment-transaction costs for consumers, small businesses, and nonprofits.
- Digital-currency firms must prioritize addressing and mitigating AML risks, given current intense scrutiny from U.S. regulators and law enforcement.
- To address these risks, digital-currency firms should:
  - Register with FinCen and obtain licenses from applicable state regulators of money transmitters
  - Establish strong AML programs
  - Collaborate with other digital-currency firms to develop information-sharing mechanisms on user identities, so that digital-currency transactions remain private but are no longer anonymous
  - Develop protocols to facilitate prevention of transactions involving certain users
- The industry should establish industrywide AML standards and, in time, a self-regulatory organization to oversee industry adherence to standards.
- Banks providing services to digital-currency firms should conduct careful due diligence, including testing the firm's AML controls.
- Digital-currency firms should consider carefully how to:
  - Convince customers of the security of both the currency itself and firm's own services
  - Navigate the possibility of Regulation E being applied to their transactions
  - Anticipate treatment of digital currencies by securities and derivatives regulators

- Growth in trading of bitcoins against fiat currencies, fueled both by its general increase in value against fiat currencies and recent market volatility.[4] Daily volume on the major exchanges now averages more than $5 million.

The other important development was the recent indictment of Liberty Reserve, a centralized digital currency that appeared to have been set up with the express purpose of facilitating — and profiting from — money laundering. While Liberty Reserve is not representative of digital currencies, it has heightened law enforcement and regulatory scrutiny on the potential for digital currencies to fund illegal activity. The U.S. Department of Homeland Security recently targeted illegal money transmission at Mt. Gox, a Bitcoin exchange, and state regulators in California, New York, and Virginia have issued orders requiring certain digital-currency firms to cease illegal money transmission.

It appears many digital-currency firms may have underestimated their regulatory obligations, the anti-money-laundering risks presented by their business models, and the degree of law-enforcement concern surrounding those risks. The U.S. government's action to force changes in international wire-messaging practices of the Society for Worldwide Interbank Financial Telecommunication demonstrates that U.S. authorities can and will require financial institutions to understand the identity of both parties to their financial transactions. The digital-currency industry should expect the U.S. government to hold firms to a similar standard and plan accordingly, which is made more challenging by the ability of users to store and send many digital currencies without using the services of a financial institution.

[4] Most notably, bitcoins reached a high of $230 at the height of the Cyprus crisis and fell to $68 within a week.

Because decentralized digital currencies, including Bitcoin, lack a central administrator, regulators and law enforcement are left to pursue public-policy objectives through oversight of those firms that enable others to trade or transact in them. Early indications are that many U.S. regulators and law enforcement authorities would welcome further development of the market through a group of digital-currency firms committed to strong AML processes and cooperation with authorities.

A fully offshore digital-currency industry still poses substantial money-laundering risks to the U.S. government (for example, in relation to drug payments); a thriving onshore industry leading the way towards better industrywide AML standards and controls that in turn strengthen industry practices globally presents the best opportunity to reduce these risks. In this respect, the entertainment industry's experience with copyright laws may be a reasonable guide: As authorities sought to enforce copyright law, they generally found it more effective to embrace and regulate distributed technologies than to try to shut them down.

The Potential of Digital Currencies

One might reasonably ask whether the game is worth the candle: Do digital currencies offer a legitimate public benefit? Assuming the industry can resolve the serious AML issues it faces, the answer clearly is yes.

Digital currencies have potential to offer payment options that are significantly cheaper than current alternatives available to consumers, small businesses, and nonprofit organizations. The longer-term cost advantage derives in large part from having fewer intermediaries to compensate. In the shorter term, the irreversibility of transactions, in particular the absence of error and dispute resolution, also lowers costs. Transaction costs for bitcoin-to-bitcoin transactions are typically around one cent. In the U.S., merchants can already accept bitcoin and receive Automated Clearing House payments in dollars for a fee of approximately 1%. Future adoption of digital currencies by mainstream financial institutions could give consumers an inexpensive method of transacting without having to hold a balance in the currency. This would mean a consumer would have no more need to understand the inner workings of the digital currency than the Automated Clearing House's transaction-processing systems. The founders of Ripple, a second-generation digital currency in late-stage development, explicitly envision the main purpose of the currency as a means to the end of facilitating payments in other currencies.

Digital currencies offer great potential for increasing efficiencies in areas such as small intercurrency transactions and remittances. The World Bank estimates that transaction fees are roughly 7% of the $500 billion global remittances market. Digital currencies also offer the potential for greater financial inclusion, particularly in increasing access to affordable payment options in the developing world, especially in applications using SMS technology.

Although the combination of digital currency and remittances may sound toxic from an AML perspective, regulators and law enforcement may eventually appreciate the robust digital trail that these transactions create. Most digital currencies already include a public ledger that records every single transaction. A digital-currency transmission system that also provides firms and law enforcement access to reliable counterparty information for all transactions would arguably have greater transparency than any major payments networks in use today. Indeed, the combination would be sufficiently powerful to require careful thought from firms and regulators alike about appropriate privacy controls.

A Bitcoin Comparison

Suppose a U.S. citizen wanted to rent a vacation house in Europe. This diagram compares some alternative methods by which a $1,000 downpayment could be sent. Even at this early stage in Bitcoin's development, the total monetary cost to the sender and recipient of transacting using bitcoin compares favorably to more traditional alternatives. The diagram also shows the potential for the sender to transmit bitcoins to the recipient without use of an intermediate financial institution. This presents novel AML issues that governments and digital-currency firms will need to address.

Sender

Bank Wire (SWIFT)
Sender provides bank with required information (recipient name, address, bank, account number, etc.).

Credit Card
Transaction details and the sender's credit card information is sent to the acquiring bank through the recipient's gateway service or payment processor.

Bitcoin
Sender adds money to a unique Bitcoin wallet for specific transaction.

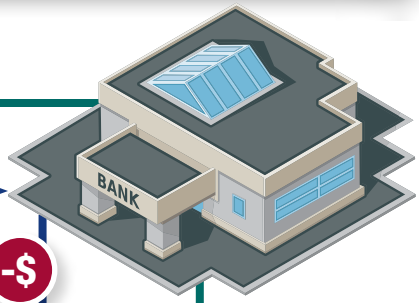
-$ 0.5%–1.0% fee to transact in and out of Bitcoin

Sender uses a Bitcoin client, which may be provided by a financial institution or operated on the sender's own computer, to initiate transfer. Distributed network of computers verifies transaction and credits the recipient.

-฿ Typical transaction fee ±$0.01; can be free

-€ 0.5%–1.0% fee to transact in and out of Bitcoin

Recipient



-$ Sender charged up to a 3% exchange conversion fee (free on some cards).

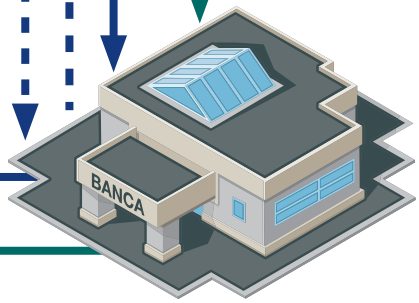
-$ Sender charged ±$40 fee for international wire transfer.

The acquiring bank sends a request through the card association to the issuing bank to confirm fund availability.

-€ Recipient charged international acquirer and interchange fees totaling ±2%.

Institution sends transaction information and instructions via SWIFT network to recipient's bank. The transaction may include intermediate correspondent institutions.

-€ Recipient may incur additional fees and exchange rate spreads from intermediate correspondent institutions and/or the recipient bank.



Estimated Total Cost For $1,000 International Transfer from USD to EUR

- Bitcoin: ±$15
- Credit Card: ±$50
- Bank Wire: ±$40-$80

How the Digital-Currency Industry Can Address AML Risks

Digital currencies will reach their potential only if the industry acts quickly to reduce AML risk. Three actions are especially necessary, of which two can be taken at the firm level, while the third requires coordination across the industry.

DEVELOP STRONG BSA/AML PROGRAMS

Regulators and law enforcement will expect firms to develop and implement Bank Secrecy Act/AML and sanctions programs commensurate with the risks of digital-currency transactions. The Financial Crimes Enforcement Network has set out the standards applicable to money transmitters in its BSA/AML Examination Manual for Money Services Businesses,[5] but digital-currency firms should consider two additional factors:

- **Know Your Customer** — The FinCen manual states that "internal controls should provide for…verification of identity," but offers little specific guidance on how firms should identify and verify their customers. Given the risks inherent in digital-currency transactions, firms can demonstrate compliance by voluntarily imposing bank-level standards for customer identification and verification, and enhanced due diligence for certain groups of customers.

- **Sanctions** — FinCen's manual does not detail the steps firms must take to comply with Office of Foreign Assets Control sanctions. Firms need strong systems and controls to prevent them from processing transactions involving customers or other parties subject to OFAC sanctions, as well as to comply with OFAC reporting requirements.

An industry initiative to develop AML standards applicable to digital currencies would benefit all digital-currency firms seeking to develop strong BSA/AML programs, and demonstrate industrywide commitment to compliance to regulators and law enforcement. Better still, the DATA initiative contemplates the establishment of a self-regulatory organization that would develop external validation of compliance with laws and regulations, as well as adherence to best practices. An SRO, which would supplement rather than replace FinCen and state oversight, would also help the industry work with regulators on difficult questions, such as how to apply the provisions of the "Travel" rule[6] in relation to digital-currency transactions.

GET NECESSARY REGISTRATION AND LICENSES

FinCen's March guidance on treatment of digital currencies[7] suggests that regulators and law enforcement will in most cases treat any firm offering digital-currency exchange, brokerage, or transaction-processing services as a money transmitter. Firms can comply with related requirements by registering with FinCen and applying for necessary state licenses, or by acting as the agent of a registered and licensed firm. While registration, licensing, and establishing an agency relationship do not by themselves reduce AML risk, they do establish a cooperative tone with regulators and enable government oversight of firms' compliance programs.[8]

---

[5] http://www.fincen.gov/news_room/rp/files/MSB_Exam_Manual.pdf
[6] http://www.fincen.gov/news_room/rp/advisory/html/advissu7.html
[7] Application of FinCen's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. FIN-2013-G001.
[8] In the case of an agency arrangement, regulators can examine the adequacy of the registered money transmitter's BSA/AML program and the quality of its agent oversight.

Given the cost of multistate licensing, availability of cost-effective agency arrangements would aid start-ups and promote continued innovation. However, money transmitters and other financial institutions providing agency services to digital-currency firms should expect enhanced regulatory scrutiny of their own BSA/AML programs and agent-oversight arrangements. Regulated firms that cannot demonstrate strong risk-management processes invite regulatory action requiring them to exit higher-risk businesses. Digital-currency firms should therefore conduct careful reverse due diligence on a regulated firm's compliance program and regulatory relations before relying on an agency arrangement.

The costs of regulation may tempt some digital-currency firms to argue that the law does not require registration or licensing, but absent regulatory concurrence, such firms deploy these arguments at their peril. Regulators and law enforcement are unlikely to tolerate any efforts to exploit gray areas or loopholes. In the words of one law enforcement official, "the tie will not go to the runner." Firms that believe they have a cast-iron case that they do not transmit money should address that argument in writing with FinCen and relevant states rather than hoping to fly under the radar.

That is not to deny firms have faced genuine uncertainty about the application of money-transmitter laws to digital-currency exchanges. Before FinCen issued its guidance, many firms reasonably relied on legal advice that they need not pursue FinCen registration or state licensing. And the FinCen guidance itself only applies to federal law, leaving considerable questions concerning the applicability of state laws to digital currency. State regulators and the industry would both benefit from dialogue that clarifies how state laws apply to digital currency. While noncompliance with money-transmitter laws is extremely serious, the genuine uncertainty provides a strong argument against punitive actions for firms that are proactive in their state regulatory outreach and move quickly to comply with state laws.

DEVELOP INFORMATION-SHARING MECHANISMS ON USER IDENTITIES

The measures just described do not sufficiently mitigate the AML risks posed by the anonymity afforded to digital-currency users. Effective AML compliance requires firms not only to Know Your Customer but also to Know Your Counterparty. Without information on their customers' counterparties, digital-currency firms will not be able to monitor transactions or screen for sanctions compliance to the standards expected of regulated financial firms. Mitigating this risk requires development of information-sharing mechanisms that allow digital-currency firms access to verified information on their customers' counterparties when needed. It may also require the ability to block transactions with identified bad actors.

Developing these mechanisms takes time, and presents several major challenges. Providing access to verified information about all transaction parties to digital-currency firms will require new protocols to supplement existing transactional information, or the development of an information-sharing database that allows digital-currency firms to identify users. Given that many digital-currency users transact from wallets stored on their own computers without using any firm's services, any solution must encompass users not associated with a particular firm. The industry could achieve this by making a Web-based verification service available to such users.

Of course, this kind of information sharing raises legitimate privacy concerns, especially when combined with the richness of transaction data available from public ledgers. The industry will need

to balance AML controls with best-practice privacy controls that assure customers that their identities and transactions will remain private even without anonymity. This could involve the provision of identity-management services by digital-currency firms or trusted third parties, with user information not generally included in transaction data and disclosed only in certain circumstances. Even then, such steps (as well as other aspects of effective AML compliance) will predictably offend some users who now use digital currencies for legitimate purposes. Development of such mechanisms may prompt greater use of measures — such as use of mixing services and multiple addresses from both money launderers and some legitimate users — to try to mask the source of funds. In the longer term, therefore, the industry may need to develop ways to prevent transactions involving users or funds that firms cannot adequately verify.

Given regulatory and law enforcement concern, leading firms would benefit from a public commitment to address these difficult issues and the expeditious formation of credible industry initiatives to address them. If the industry can move forward while engaging regulators and law enforcement, it can make a strong argument that its initiative will lead to good public-policy outcomes and therefore should be given time to get controls in place.

Implications for Banks

Digital currencies present both opportunities and threats to banks. While digital currencies give banks opportunities to offer new services to existing customers, some will cut into existing profitable ones. The digital-currency firms that form successful partnerships with banks to offer services will be those that offer a business model that provides clear benefits over the status quo to banks and their customers alike.

Banks also have opportunities to provide banking services to digital-currency firms. As detailed in a past Promontory Sightlines InFocus,"Regulatory Convergence on Vendor Management," regulatory expectations for banks' third-party oversight continue to grow.[9] Banks providing services to digital-currency firms, such as access to the ACH network, should conduct careful due diligence on the firms, including detailed review of their:

- BSA/AML programs
- Information-security and privacy programs
- Marketing, disclosures, and other consumer materials
- Chargeback rates

Other Challenges Facing Digital Currencies

AML risks are merely the most immediate regulatory challenges facing digital-currency firms. Those firms that successfully meet regulatory expectations for AML compliance must address a wider array of regulatory and public-policy concerns before digital currencies can fulfill their considerable potential.

[9] http://www.promontory.com/News.aspx?id=2774

INFORMATION SECURITY

Consumers and regulators must be confident that both digital currencies and firms offering digital-currency services do not present heightened information-security risks. The industry will need to persuade potential users that each currency's cryptography and transaction validation can withstand external attack. Distributed digital currencies face particular challenges in gaining widespread trust, as there is no legal entity to offer recourse to users. The industry must also overcome negative perceptions resulting from security breaches that have already occurred at individual firms, and demonstrate that firms have fully addressed the control weaknesses that allowed those breaches.

CONSUMER PROTECTION

Any digital-currency exchange operating in the U.S. that achieves the volume to which it aspires will soon confront the possibility of compliance with the Electronic Fund Transfer Act and Regulation E, which impose on certain payment-service providers significant obligations related to error resolution and limited liability for unauthorized transfers. Indeed, consumer protection could arise as a strategic question even before it becomes a regulatory imperative, as consumers may prove wary of adopting new payment mechanisms that do not offer the same protections they enjoy with existing options. The same irreversibility of digital-currency transactions that many in the digital-currency industry value for its efficiency could make it prohibitively expensive under existing protocols to provide limited liability and dispute-resolution protections that most consumers now have with their banks and credit card companies. Digital-currency firms should contemplate supplementing existing software to reverse transactions, provide escrow services, or otherwise make consumers whole in cases where errors or unauthorized transfers occur, perhaps as a value-added service. Proactive thinking, as well as engagement with regulators to understand the extent EFTA and Regulation E requirements apply to digital-currency transactions, will facilitate quick industry response if it eventually becomes clear that either regulatory concerns or market pressures require transaction reversibility.

OTHER U.S. REGULATORS' TREATMENT OF DIGITAL CURRENCIES

To date, the U.S. regulatory authorities most focused on digital currencies are those focused on money-services businesses, which emphasize licensing, AML compliance, customer protection, and information-security issues. Just over the horizon, however, lurk additional regulators whose concerns will predictably increase as use of digital currencies grows. In the U.S. context:

- The Commodity Futures Trading Commission and/or the Securities and Exchange Commission could seek to exert more general regulatory authority over digital currencies. Commissioner Bart Chilton announced in May that he had asked CFTC staff to explore whether retail customers needed more protection on Bitcoin transactions.

- Even if the CFTC does not assert broad regulatory authority over digital currencies, growing demand for forwards and other digital-currency-based derivatives could drive the CFTC and the National Futures Association to treat a given digital currency, or all of them, as a commodity or currency. Either interpretation could lead to CFTC and NFA regulation of entities providing nonspot transactions to the retail sector.

- Any plans for mutual or exchange-traded funds relating to digital currencies or digital-currency firms would, of course, fall under the purview of the SEC.

Digital Currencies: A Brief FAQ

What are digital currencies?

Digital currencies are digital or electronic money not backed by a government body. Many digital currencies, including Bitcoin, are cryptocurrencies that use cryptography to create peer-to-peer, decentralized currency and payment systems. Many cryptocurrencies enable users to conduct transactions using the Internet without necessarily requiring an intermediary financial institution.

What is Bitcoin?

Launched as an open-source protocol in 2009, Bitcoin was the first cryptocurrency; the currency unit is sometimes referred to as BTC. Bitcoin's money supply is limited; only 21 million bitcoins will enter circulation, with the final bitcoin scheduled to be released in 2140. Each bitcoin may be divided into 100 million subunits. Currently, there are more than 11 million bitcoins in circulation, and their total market value as of mid-August was approximately $1.1 billion.

How does the Bitcoin system work?

The Bitcoin system leverages a complex, technical, and increasingly competitive process, called mining, that prevents fraud and system errors by validating user transactions. Every bitcoin transaction is recorded in a universal public ledger called the block chain. The block chain contains units of data called blocks; the system creates new blocks by bundling recent transactions. Bitcoin miners take each newly created block and, through a complex mathematical process, work to confirm that block in a manner that effectively validates those transactions. The miner that confirms a particular block is rewarded with a set number of newly created bitcoins, and the block chain is updated with the confirmed block. The system is designed to confirm a new block and, by extension, to issue new bitcoins, every 10 minutes.

How do people fund bitcoin purchases?

Users deposit fiat currency (e.g., U.S. dollars) with an exchange or send fiat currency to a broker. Common deposit methods include wires and the Automated Clearing House. On an exchange, users can trade at the best available rate or make limit orders. Brokers usually guarantee the rate at the time of purchase. In the reverse process, a user owning bitcoins may use an exchange or a broker to convert BTC to fiat currency deposited into the user's bank account. Brokers and exchanges charge a percentage for transactions and may levy additional fees.

How do people store and send bitcoins?

Users store bitcoins in a digital wallet hosted by a third-party Bitcoin client or on their own computer. A wallet may contain one or more addresses. An address is an alphanumeric string, such as 1CC3X2gu58d6wXUWMffpuzN9JAfTUWu4Kj, and is composed of a unique private key, akin to a password known only to the user, and public key, akin to a username and known to any Bitcoin user. User A transfers bitcoins to User B through User B's address (some users create a new address for each transaction). User A attaches his public key to the transaction and uses his corresponding private key. The transaction is then broadcast to the Bitcoin system. The public keys attached to the transaction allow miners to validate its legitimacy. Some bitcoin-to-bitcoin transactions are free, while others require a transaction fee (in bitcoin) to encourage timely processing by miners. The minimum transaction fee is roughly a penny, with higher fee levels attracting faster processing.

Commodities, derivatives, and securities regulators worldwide will need to confront similar issues as the digital-currency market grows. More speculatively, some jurisdictions could consider regulating digital currencies as securities. In all of these cases, engagement with regulators — both in the U.S. and globally — will reduce the risk of unpleasant surprises.

Conclusion

Digital currencies offer the potential prize of cheaper and faster payments for many consumers and organizations, including many poorly served by existing options. From the perspective of law enforcement and regulators, successfully addressing the Know Your Counterparty issue would mean digital currencies offer a stronger basis for both preventing and identifying money laundering than most, if not all, existing payment networks. The industry and consumers will only realize these benefits, however, if digital-currency firms prioritize AML and other important public-policy challenges posed by digital currencies. This will require hard work, leadership, and ingenuity from the industry and regulatory authorities alike.

Daniel Bufithis-Hurie and Daniel Bulaevsky contributed to this article.

Contact Promontory

For more information, please call or email your usual Promontory contact, or:

Konrad Alt
Managing Director, San Francisco
kalt@promontory.com
+1 415 986 4160

William Haraf
Managing Director, San Francisco
wharaf@promontory.com
+1 415 986 4660

Doug Harris
Managing Director, New York
dharris@promontory.com
+1 212 365 6568

Simon McDougall
Managing Director, London
smcdougall@promontory.com
+44 207 997 3456

Gary Owen
Director, New York
gowen@promontory.com
+1 212 365 6565

Adam Shapiro
Director, San Francisco
ashapiro@promontory.com
+1 415 321 6404

David Stein
Director, Washington, D.C.
dstein@promontory.com
+1 202 384 1183


To subscribe to Promontory's publications, please visit promontory.com/subscribe.aspx


Follow Promontory on Twitter @PromontoryFG

Global Offices

ATLANTA
Midtown Proscenium Center
1170 Peachtree Street, Suite 1200
Atlanta, GA 30309
+1 404 885 5741

BRUSSELS
Promontory Financial Group – Brussels Branch
Square de Meeûs 35
1000 Brussels, Belgium
+32 2 893 97 61

DENVER
1999 Broadway, Suite 1800
Denver, CO 80202
+1 720 612 5000

DUBAI
Promontory Financial Group, LLC
Emaar Square
Building 4, Office 204
Sheikh Zayed Road
P.O. Box 53854
Dubai, UAE
+971 4 445 15 55

HONG KONG
Promontory Financial Group China Ltd
Level 10, Central Building
1-3 Pedder Street
Central, Hong Kong SAR, China
+852 3975 2901

LONDON
Promontory Financial Group UK Ltd
2nd Floor, 30 Old Broad Street
London, UK EC2N 1HT
+44 20 7997 3400

MILAN
Promontory Financial Group Italy S.r.l.
Via Alessandro Manzoni, 3
20121 Milan, Italy
+39 02 7262 2100

NEW YORK
280 Park Avenue, 40th Floor West
New York, NY 10017
+1 212 365 6565

PARIS
Promontory Financial Group France SAS
28 Boulevard Haussmann
75009 Paris, France
+33 1 44 79 17 20

SAN FRANCISCO
Spear Tower, Suite 4100
1 Market Plaza
San Francisco, CA 94105
+1 415 986 4660

SINGAPORE
Promontory Financial Group Australasia, LLP
260 Orchard Road
#19-01 The Heeren
Singapore 238855
+65 6410 0900

SYDNEY
Promontory Australasia Sydney Pty Ltd
Level 32, 1 Market Street
Sydney, NSW 2000, Australia
+61 2 9275 8833

TOKYO
Promontory Financial Group
Global Services Japan, LLC
Teikoku Hotel Tower 9F
1-1-1, Uchisaiwaicho
Chiyoda-ku, Tokyo 100-0011, Japan
+81 3 3519 1400

TORONTO
Promontory Financial Group Canada ULC
TD Centre, P.O. Box 326
77 King Street West, Suite 3720
Toronto, Ontario M5K 1K7, Canada
+1 416 863 8500

WASHINGTON, D.C.
801 17th Street, NW, Suite 1100
Washington, DC 20006
+1 202 384 1200

PROMONTORY

Promontory is a leading strategy, risk management, and regulatory compliance consulting firm for the financial services industry. Promontory's professionals have deep and varied expertise gained through decades of experience as senior leaders of regulatory bodies and financial institutions. Promontory assists clients in meeting regulatory requirements and in enhancing governance, risk management, strategic plans, and compliance programs.

Promontory Financial Group, LLC
801 17th Street, NW, Suite 1100, Washington, DC 20006 Telephone +1 202 384 1200 Fax +1 202 783 2924 promontory.com