Hong Kong Begins Gearing Up to Relaunch $3 Billion REIT

- The drama began last year as the government was marketing the REIT. Lo Siu Lan (盧少蘭), a welfare recipient, argued that the privatization could raise rents and, in turn, prices in local shops, violating the city's housing code.
- Even before a legal challenge to the world's biggest real estate investment trust is resolved, Hong Kong is quietly marshaling advisers, lawyers and underwriters to prepare to relaunch the US$3 billion Link real estate investment trust.
- The sale of the Link REIT is important not just to the finances of the city's housing authority but also for the development of Hong Kong's market in property trusts.

Source: AWSJ (July 14 2005 – M1)

Hong Kong Begins Gearing Up to Relaunch $3 Billion REIT

- Hong Kong is a REIT laggard among Asian markets, without a single traded trust. Meanwhile, property trusts in other Asian markets, from Tokyo to Singapore, have soared this year. The market value of REITs in Asia excluding Australia has more than quadrupled to US$27.5 billion in the past two years.
- In May, Hong Kong changed its rules for the trusts, opening the way for REITs to include investments outside Hong Kong as well as raising the cap on the debt that a trust can have.
- A look at the Asian REIT market

Country	Market Cap in billions of $	# of REITs	% of equity market	% of real estate
Japan	21.35	18	1.0%	4.5%
Singapore	5.45	5	1.8%	17.0%
Korea	0.65	7	0.2%	1.3%
Malaysia	0.07	4	0.6%	0.6%

Source: AWSJ (July 14 2005 – M1)

Let's Stop ID Theft, Not Just Talk About It

- In the current ID-theft debate, however, government and industry may have missed the point. Sure, consumers need to know when their information is compromised. But the real opportunity – and fiduciary obligation – for financial institutions is to do better at fighting ID theft before it happens.
- The simple fact that a growing number of carriers now underwrite identity-theft insurance means the financial system will accept the risk. This is also means we all run the greater risk of accepting ID theft as a way of life, with insurance as the best hedge.
- However, a financial institution's most important product is trust. To maintain that trust, banks need stronger weapons to meet the new challenges of industrialized fraud.

Source: American Banker Online (July 8, 2005)

Let's Stop ID Theft, Not Just Talk About It

- Banks need to better integrate knowledge and information at all channels – branch, online, telephone, etc. – to create a fraud-monitoring "ecosystem." They have great resources to fight ID theft; the trick is to unify the power of many separate fraud-prevention tools they use today.
- People are willing to pay for stronger security and identity protection, even if that means leaving their current banks to get it.
- According to the Unisys survey, more than half of U.S. households would consider changing to financial institutions that offer additional detection and alert services. The research firm Financial Insights found in March that 6% of consumers have already made the switch due to ID theft.

Source: American Banker Online (July 8, 2005)

Threats from Fraudulent Bank Web Sites

- Web-site spoofing is a method creating fraudulent Web sites that look similar, if not identical, to an actual site, such as that of a bank. Customers are typically directed to these spoofed Web sites through phishing schemes. Once at the spoofed Web site, the customers are enticed to enter information such as their Internet banking username and password, credit card information, etc.
- Spoofing exposes a bank to strategic, operational, and reputational risks; jeopardizes the privacy of bank customers; and exposes banks and their customers to the risk of financial fraud.

Source: OCC Bulletin (July 1, 2005)

Threats from Fraudulent Bank Web Sites

- A bank can help minimize the impact of a spoofing incident by assigning certain bank employees responsibility for responding to such incidents and training them in the steps necessary to respond effectively.
- If a bank's Internet activities are outsourced, the bank can address spoofing risks by ensuring that its contracts with its technology service providers stipulate appropriate procedures for detecting and reporting spoofing incidents, and that the service provider's process for responding to such incidents is integrated with the bank's own internal procedures.
- Banks can use customer education programs to mitigate some of the risks associated with spoofing attacks. In addition, because the attacks can exploit vulnerabilities in Web browsers and/or operation systems, banks should consider reminding their customers of the importance of safe computing practices.

Source: OCC Bulletin (July 1, 2005)

Threats from Fraudulent Bank Web Sites

- To respond to spoofing incidents effectively, bank management should establish structured and consistent procedures. These procedures should be designed to close fraudulent Web sites, obtain identifying information from the spoofed Web site to protect customers, and preserve evidence that may be helpful in connection with any subsequent law enforcement investigations.
- If a bank is the target of a spoofing incident, it should promptly notify its OCC supervisory office and report the incident to the FBI and appropriate state and local law enforcement authorities. Banks can also file complaints with the Internet Fraud Complaint Center, a partnership of the FBI and the National White Collar Crime Center.
- In addition to reporting to the bank's supervisory office, there are other less formal mechanisms that a bank can use to report these incidents and help combat fraudulent activities. For example, banks can use "Digital Phishnet", which is a joint initiative of industry and law enforcement.

Source: OCC Bulletin (July 1, 2005)

While this might reflect in part weaker incentives, given their relatively more stable revenues and higher margins, it has prompted the attention of regulators.