My hope is that this essay will be a *starting point* for further, positive discussion as the topic of information security breaches and reputational risk is becoming of paramount importance.

How It's Difficult to Ruin a Good Name:

An Analysis of Reputational Risk

by

Kenneth F. Belva, CISSP

September 19, 2005

http://www.ftusecurity.com

I. Introductory Remarks

Good afternoon.

While most of this presentation was written on Starbuck's Pumpkin Spice Lattes, if there are any errors in the analysis they are mine as much as I would like to blame the lattes.

The title of my presentation is:

How It's Difficult to Ruin a Good Name: An Analysis of Reputational Risk.

II. Project and Thesis

After there were a number of insiders at Bank of America and Wachovia who illegally sold non-public information to an outside organization, I found myself in two conversations: the first was whether or not such a thing is likely to occur again [1]. My argument was that since risk cannot be reduced to zero, there is a likelihood of another incident. I further told this individual that it would most likely happen at a major institution. This individual, on the other hand, assumed that if an institution is large, the proper controls must be in place and that such an incident would not happen again. Sure enough Citigroup (CitiFinancial) and UPS lost 3.9 million customer records a few weeks later [2]. I effectively won the argument. Although, I did not expect to win so soon.

The point of the first story is this: it can happen to you at any time, no matter who you are, no matter what size.

The second discussion came out of the first. While I spoke to my friend Sam (who is not the same person with whom I had the first conversation), I remarked: "Sam, you know there were these recent security events and I really didn't see much fallout from them. We did not hear reports of accounts closing at these institutions. We did not hear about a single lawsuit filed against these companies." I said further, "There really didn't seem to be much collateral damage from these high profile security breaches. Isn't this the opposite of what we'd expect? Wouldn't we expect a loss of consumer confidence? Wouldn't we expect a loss of institutional confidence?" Needless to say I switched from my previous presentation topic to reputational risk.

The second story leads to my current research and this presentation: What is the impact of an information security breach both monetarily and on one's reputation if the breach is publicly disclosed? And, just as important, why does it happen in the way that it does? What are the factors that lead to the results (outcomes)? This becomes especially relevant as most States are beginning to pass laws similar to California's SB1386.

The title of my presentation -- How It's Difficult to Ruin a Good Name -- may have hinted at my conclusion.

Perhaps some of you are skeptical. I know I was before I completed my research. Perhaps you even know of a case or two that seem to contradict my hypothesis. All I ask is that you withhold judgment until after the evidence is presented.

The results of my research (this presentation) ultimately seek to instruct. After looking at why some corporations are effected while others are not, the research aims to create a procedural framework in the case of an information security breach. Although unintended, the research answers where best to place allocated security capital within the technical infrastructure. In addition – and to our benefit -- while the reputational risk results are novel, the procedure on how to deal with these situations fits our intuition.

I think it is worth mentioning something explicitly: Despite the conclusion, I am not advocating that one should disregard best practices, security standards or anything of that nature. It is due to these practices that organizations are better protected and can properly respond should an incident occur.

II Methodology

My method is to take the only publicly visible measure of confidence in a corporate institution and determine if the impact is significant after an incident is publicly disclosed. In short, I am doing an analysis of a company's stock price.

I correlate the behavior of the equity with information security incident disclosure. The source of the disclosure is either the corporation itself or the media at large. I then look at some facts of the case and suggest an answer to why things perhaps went the way they did and not otherwise.

There are limitations to my analysis and I will be up front about them here: First, there may not be enough cases to conclude with certainty that future events will echo past cases. We can make a reasonable assumption that it might, but we don't know for sure. Second, it is difficult to determine other types of loss (such as number of accounts closed, etc.) without some internal corporate data. In short, I do not have access to that information. And, if I had access, the odds are I would not be allowed to report on it publicly. Finally, it may the case that those with other analytical tools may calculate and interpret the data differently.

That said, I would consider revising my conclusion once more data is gathered. *I see this paper as a starting point for further discussion.* At this point in time, I think the data is suggestive enough to provide an accurate picture of how we should understand reputational risk going forward.

III. Evidence

The goal in this section is to simply point out facts. I am not looking to reach a conclusion, except in a rare case were the facts taken together point to something more constructive that will be used later.

So, lets get down to it.

We will examine the following companies' stock prices: Polo Ralph Lauren, DSW Shoe Warehouse (RVI), UPS, Citigroup, Bank of America, Wachovia, Choicepoint and Time Warner.

I've spent quite a bit of time trying to find the best way to present the data. It seems to me that the best way to break things up are from a macro perspective (long term trends) and micro perspective (short term trends).

Note that the the '**' are the dates of the reported incident, usually media reports. A 'D' is for a dividend that was paid. As we look at the stock charts, some are obscured by the price box: the individual who printed the graphs told me that is was not possible to move these boxes. All historical stock prices were take from http://finance.yahoo.com.

Micro Trends

Polo Ralph Lauren (RL)

Date	Volume	Close	Increase (+) / Decrease (-)	*% of +/-*
04/13/05	445400	38.46		
04/14/05	603600	37.18	-1.28	3.32%
**04/15/05	1320700	35.78	-1.4	3.77%
04/18/05	729900	35.95	0.17	0.48%
04/19/05	593200	36.73	0.78	2.17%
04/20/05	366900	36.45	-0.28	0.76%
04/21/05	348200	36.86	0.41	1.12%

In the case of Polo, we see the reported incident occurred on Friday, April 15, 2005. There was an immediate drop in market value of 3.77%. But, balance this with the fact that the day before there was a loss of 3.32% and the day after there was a gain of .48%. Perhaps worth noting is that the third day – May 19, 2005 – there was a gain of 2.17% to put the stock price higher than before the incident occurred.

DSW Shoe Warehouse (RVI – Retail Ventures Incorporated)

DSW March Press Release

Date	Volume	Close	Increase (+) / Decrease (-)	*% of +/-*
03/07/05	18500	7.36		
**03/08/05	19,900	7.30	-0.06	0.82%
03/09/05	47,300	7.30	0	0.00%
03/10/05	36,600	7.46	0.16	2.19%
03/11/05	21,200	7.32	-0.14	1.88%
03/14/05	915,200	9.20	1.88	25.68%
03/15/05	439,100	8.97	-0.23	2.50%

DSW April Press Release

Date	Volume	Close	Increase (+) / Decrease (-)	*% of +/-*
04/15/05	220,400	9.28		
**04/18/05	113,300	9.51	0.23	2.48%
04/19/05	119500	9.45	0.06	0.63%
04/20/05	124800	9.30	-0.15	1.59%
04/21/05	130600	9.63	0.3	3.55%
04/22/05	124700	9.42	-0.21	2.18%
04/25/05	238900	9.58	0.16	1.70%

DSW Shoe Warehouse breach resulted in two press releases: one in March and the other in April.

In the first case of DSW Shoe Warehouse, we see that there is a .82% loss on the day of the press release. The following day there is no loss. The stock gains 2.19% two days later.

In the second case of DSW Shoe Warehouse, we see that there was a gain of 2.48% on the day of the press release. The following day the stock gained another .63%. Two days after the second press release there is a decline of 1.59% although the price of the stock remains higher than before the second press release was published.

UPS (UPS)

Date	Volume	Close	Increase (+) / Decrease (-)	*% of +/-*
06/03/05	2294000	72.82		
**06/06/05	1758000	72.86	0.04	0.05%
06/07/05	2,200,800	73.02	0.16	0.22%
06/08/05	2144400	72.36	-0.66	0.90%
06/09/05	6074900	71.2	-1.16	1.60%
06/10/05	2554100	70.96	-0.24	0.34%
06/13/05	2872100	70.17	-0.79	1.11%

In the case of UPS, there was a gain on the day of the incident of .05%. The next day there was a gain of .22%. The stock falls and continues to fall after the second day of the reported incident.

Citigroup (C)

Date	Volume	Close	Increase (+) / Decrease (-)	*% of +/-*
06/01/05	14724300	47.72		
**06/02/05	8021000	47.71	-0.01	0.02%
06/03/05	9641600	47.56	-0.15	0.31%
**06/06/05	6015900	47.69	0.13	0.27%
06/07/05	11465100	47.66	-0.03	0.06%
06/08/05	7976200	47.75	-0.09	0.19%
06/09/05	7,176,100	47.68	-0.07	0.15%
06/10/05	8,570,300	47.64	-0.04	0.08%
06/13/05	8,350,200	47.6	-0.04	0.08%

Citigroup is an interesting case. The price of the stock falls .02% on the day of their press release, June 2nd. When it hits the papers on June 6th the price of the stock rises 0.27%.

Bank of America (BAC)

Date	Volume	Close	Increase (+) / Decrease (-)	*% of +/-*
05/20/05	7617800	46.57		
**05/23/05	5728600	46.55	-0.02	0.04%
05/24/05	6,375,100	46.61	0.06	0.13%
05/25/05	6931900	46.54	-0.07	0.15%
05/26/05	6935700	46.71	0.17	0.37%
05/27/05	5211400	46.65	0.09	0.13%
05/31/05	9095400	46.32	-0.33	0.70%

Bank of America's stock fell by .04% the day of the incident announcement, and rose . 13% the day after.

Wachovia (WB)

Date	Volume	Close	Increase (+) / Decrease (-)	*% of +/-*
05/20/05	3,828,300	52.42		
**05/23/05	3396100	52.26	-0.16	0.31%
05/24/05	3,151,700	52.15	-0.11	0.21%
05/25/05	2155400	51.89	-0.26	0.50%
(D) 05/26/05	2797900	51.92	0.03	0.06%

Date	Volume	Close	Increase (+) / Decrease (-)	*% of +/-*
05/27/05	6161200	51.04	-0.88	1.69%
05/31/05	3836400	50.75	-0.29	0.57%

Wachovia's incident occurred on May 23 and we see a decline of .31% percent. The next day there is also a smaller decrease in price of .21% ('D' means a dividend was paid.)

Choicepoint (CPS)

Date	Volume	Close	Increase (+) / Decrease (-)	*% of +/-*
02/16/05	621800	45.54		
**02/17/05	1067300	44.13	-1.41	3.10%
02/18/05	1188800	43.5	-0.63	1.42%
02/22/05	3758900	39.3	-4.2	9.66%
02/23/05	3778500	41.22	1.92	4.89%
02/24/05	1357400	41	-0.22	0.53%
02/25/05	1,130,400	40.27	-0.73	1.78%

Except for a gain of 4.89% on February 23, Choicepoint's stock continuously falls (within our table). It falls 3.10% on the day of the reported incident.

Time Warner (TWX)

Date	Volume	Close	Increase (+) / Decrease (-)	*% of +/-*
29-Apr-05	25042800	16.81		
**05/02/05	11930400	16.8	-0.01	0.06%
**05/03/05	21727200	16.68	-0.12	0.71%

Date	Volume	Close	Increase (+) / Decrease (-)	*% of +/-*
05/04/05	20856900	17.28	0.6	3.60%
5-May-05	16840100	17.12	-0.16	0.93%
05/06/05	13021200	17.12	0	0
05/09/05	10428900	17.34	0.22	1.29%
05/10/05	14562000	16.98	-0.38	2.08%

Time warner drops .06% on May 2nd, the day their internal memo is released. The day it hits the papers the stock drops .71%. But it rises the next day 3.60% to a price higher than before the day of the internal memo.

Macro Trends

For the macro trends, we'll break the group the companies as follows: retail (Polo Ralph Lauren and DSW Shoe Warehouse), financial (Bank of America, Wachovia and Citigroup) and technology (Choicepoint). The other two stocks UPS and Time warner appear to be inconclusive when trying to determine the impact of a reported incident over the long term.

If we look at the long term trends of Polo Ralph Lauren and DSW Shoe Warehouse we notice that it is an upward trend. The incidents for Polo happened on April 15, 2005. The second press release for DSW Show Warehouse occurred on April 20, 2005. What this seems to suggest is that over the long term the impact of the reported breach in these cases is minimal.

If we turn to the financial sector, we notice that Citigroup tends to decrease slowly and then has this sudden dip on July 15th. Looking at Bank of America and Wachovia around the same time, July 15th, we notice that there is a decrease as well. In the Bank of America and Wachovia cases we have two large dips. The second drop in Bank of America and Wachovia correlates to a drop in Citi's stock. The second drop in price is due to a concern that this sector of the market may take a hit due to rising interest rates [3].

Neither of these two drops are due to information security breaches. We are interested in the first drop though. There is an AP story that says that Bank of America and Wachovia are foremost mentioned in a lawsuit for price fixing [4]. Bingo. A drop in price. The lawsuit could result in a one-off financial loss. Both stocks recover from the lawsuit drop until the market sector concern hits the wires.

Choice point is hit the hardest. After the price falls, it struggles to return to its previous market value over a significant period of time.

UPS and Time Warner appear to be inclusive. We cannot see any long term trends.

IV. Derivation of Laws from Case studies

Information security awareness is at its height at this point in history and this is the proper context in which to understand the facts stated in the section above. Worms, identity theft, phishing, SPAM and scams initiated through SPAM are real and generally known by the public. The public is more aware than at any other historical period about the possibilities and dangers related to mishandling information. We can assume that this knowledge will effect people's decision making.

So, here's a quick review of facts based on the of micro trends above:

1) 3/4 (75%) stocks dropped the day the information security incident was reported

2) 5/8 (62.5%) stocks has *some gain* within two days of the reported incident

[Note: These short term percentages do not include Citigroup since the stock performed in opposite directions on the press release and the media release. I have counted the DSW Shoe Warehouse twice, once for the March press release and once for the April press release.]

Here is a the result of the macro (long term) trends:

1) In the majority of cases, the stock does not seem to be effect by the reported information security breach. Other factors may influence the price, but the breach usually is not a factor, as evidenced by the retail and financial equities.

From these facts we can state our first general rule:

In the short term there may be some detrimental consequences if there is a *potential financial impact*, but over the long term we find that unless there is a true impact, the reported incident is forgotten and the stock appears to follow the larger industry trends and/or becomes impacted by other considerations.

The question is to what extent and why? To what extent is (or isn't) investor confidence shaken? In other words, why is it the case that information security incidents do not appear to have a greater impact on both investor confidence as well as the public at large? To phrase the question in financial terms: why isn't the top line effected more than it is? To poignantly highlight this phenomena we ask: If 40 million customer credit card numbers are exposed in a security breach at the credit card processor CardSystems , why do a significant number people not cancel their Visa and/or Mastercard [5]?

In order to answer these questions, it is instructive to review the cases in which there is long term damage. By isolating the cause of the long term damage, we will be able to note that it does not occur in the short term loss cases.

The first long term loss case is Choicepoint; the second case is CardSystems. How are these two cases alike? Financially we noticed Choicepoint's stock was down for a significant period of time. The reason for the long term loss was that their top line was affected: Choicepoint changed and dropped some of their information products as a result of their breach[6].

Let's turn to the Cardsystems case. Unfortunately, neither Mastercard, Visa or CardSystems is represented by an equity we can analyze. But, we can discuss the incident. Cardsystems is a processor of data, specifically credit card transactions. The data, their core business, was compromised. In the case of CardSystems, although they do not have stock, one of their major providers no longer use their service: Visa dropped them as a card processor service[7]. (Mastercard still uses CardSystems.)

With these two cases in mind we can move from the general, short term case of potential financial impact to a derived rule:

If the security incident directly effects your *core business* – the service or products you provide – an information security incident may really hurt you. Both cases directly effected the top line.

This rule may even apply to cases that are not tied to the information security field. The primary example here is Arthur Anderson. The firm's integrity was destroyed when the reputation around their core business was tarnished through a conflict of interest.

In the cases were there was a temporary loss or no loss at all, it appears that the breach was not in an area that effected the core business. In other words, even though Citigroup and UPS lost 3.9 million customer records, Citigroup was still able to lend money and UPS could continue shipping packages..

I am willing to leave an open hypothesis on the table: The greater the financial impact or potential financial impact from the information security incident, the greater the reputational damage; the less the financial impact or potential financial impact from an information security incident, the less the reputational damage.

We see that the incident effected the processor of Visa and Mastercard transactions, but was Visa or Mastercard effected? I could not find reports to confirm that they were. While I do not have any hard evidence, based on the Bank of America/Wachovia and Citigroup cases, I will wager that the answer is no (or not significant). People just did not seem to stop using their Visa or Mastercard. People did not seem to close their Bank of America accounts or decide to stop banking at Citigroup.

On the assumption that the core business was not effected, how are we to understand consumer behavior? It seems to me the best way to make sense of this is twofold. Consumer behavior is effected by the amount of effort needed to make a change (first reason) combined with the extent to which people feel that their choice will make a difference (second reason). Otherwise stated: the more difficult something is to change, the less inclined someone is to

change it. I think it is instructive here to contrast the cases that were not seriously affected by a breach with that of Wendy's.

As you may recall someone claimed to find a finger in a bowl of Wendy's chili. This was a *false* incident; it was part of a scam. The claim is fraudulent, and people knew it, but the damage was done to Wendy's reputation and public image. In Q2/2005 Wendy's declared a 4% lower profit directly tied to the incident [8].

Well, there seems to be something very tangible about food and eating. Finance is more abstract. What we put in our bodies is very concrete in the mind's eye; it seems to me that someone would be hard pressed to make the same case for someone's credit limit. If we believe that what one chooses to put in one's body is more easily grasped by the mind, than it is reasonable to say that changing what and where one eats is more tangible than switching financial products. With consumers being somewhat health conscious, people feel that where they eat makes a difference to their lives. (This is the second point.)

It is also very easy to choose where to eat. If there are two fast food restaurants in the near vicinity and one has had some bad press, it seems just as easy to stop at the other fast food establishment, especially if it is across the street from the one that received the bad press. (This is the first point.)

Decisions about controlling our personal information are different than food. Once it is keyed into a computer system, most people (including myself) cannot follow all the systems through which our information travels. In fact, we cannot even guarantee that when we call to apply for a new credit card, the information is keyed by the company to which we are applying. Outsourcing and third party service providers may have created situations where data is no longer stored only at the company with which I do business. From personal experience, I know that my primary bank has outsourced its online billpay service. The online billpay site stores my credit card information, my other institutional checking and savings account numbers as well as my investment account information. To further complicate matters, my information is probably

replicated to disaster recovery sites for all these systems. Is it protected there to the same degree as the core systems?

Somehow it seems that controlling my information is much more difficult that controlling where I eat. And in the end might not be worth it anyway: Before the Cardsystems incident was reported, if I were to switch from Visa to Mastercard, I'd be in the same position since they both used CardSystems. And what if I had both cards?

Before I head into the conclusion I would like to mention something that I do not want to leave on the drawing board. While it may not fit in the context of the previous discussion, it is interesting to note none-the-less:

There is another consequence to the reputational theory presented above. Due to the market value loss and the potential for future loss, I'd consider the reporting of an information security incident as bad news. The research suggests that the stock price may rebound if the incident does not effect the core business or the financial loss is not significant. Perhaps the old adage to “buy on bad news and sell on good news” may be applied here. Information security incidents are discrete events and the facts are usually concrete. Based on the known cases of publicly disclosed information security breaches, perhaps there is a good chance that the stock will declining in the short term and rebound soon after. In effect, it may be possible to make money off the publicly reported breach. Granted, I did not say this was an ethical thing to do, only that it seems possible to do in theory.

V. Conclusion

Contradictory to one might imagine, information security incidents may not suggest a general lack of internal controls.

It does mean that there was a specific control weakness at that particular moment, that we cannot deny.

On the condition that it was not gross negligence – and that is key, the incident is not due to negligence -- what an incident suggests is that the level of risk rose above the assumed or

projected risk at a given instant in time. Probability seems to suggest that something will happen at some point in time to someone. The larger the institution the greater the chance that something will happen. It seems to me that that is why the public tolerates it to some extent. Information security incidents are a cost of doing business: these things happen every so often.

And that is another key: every so often. The incidents are not systemic. They occur infrequently. We publicly have not had cases that were systemic in nature, yet. If Citigroup and UPS lost 3.9 million customer records every week and Bank of America's employees were found to consistently sell customer information illegally, we would most likely change our minds about where we do business.

Conventional wisdom in the information security field says, “Only put a reasonable amount of control in place: enough to reduce the risk to a tolerable level even though this will not be absolute protection. One cannot reduce the risk to zero.” And I agree: corporations do not have unlimited resources.

This is why due diligence is important. Should there be an incident, showing you tried is second to actually preventing it. Not everything can be prevented but one should protect the top line and one-offs to a reasonable degree.

As we learned from the research: the area to protect most is one's core business and that is where to focus the capital effort. Unfortunately, there is a catch here: usually the areas most vulnerable – and hence where the data is compromised – is exactly in the areas that are least protected. This is evidenced by the CardSystem case [9]. (If you doubt this, ask if your production data is used on your test systems and then follow up by asking whether the controls on the test system are as strong as production!) What this suggests is that while a good portion of capital should be allocated to protect the core business, some capital should be allocated to protected the rest of the infrastructure. This seems to fit our common sense as well.

And what should the reaction be if there is an incident?

The big corporations have the right idea and I'm taking a page from their play book.

The following steps below are suggestions and guidelines. They should not be taken as advice. Please consult a legal professional before doing any of the following. Now that the disclaimer is out of the way....

All of the steps below were taken from true cases; they were field tested. They are not listed in any particular order. These were the techniques that were used by the corporations who were effected the least by their information security incident. Past performance is not a guarantee of future results.

First, corporations such as Time Warner, Bank of America, Wachovia and Citigroup offered advice or services to help to protect their customers [10,11,12,13].

Second, Citigroup, Time Warner, Bank of America and Wachovia each said that the breach did not effect either their customers or their employees despite the information loss or disclosure [10,11,12,13]. (The abstract point here is that there will not be any financial loss by either those that had their data compromised or the corporation.)

Third: in the press release from Citigroup and internal memo from Time Warner, both corporations use the phrase "We deeply regret this incident" somewhere in the disclosure giving the statement an apologetic tone [11,12].

Fourth, a corrective action has been taken to prevent the incident from happening in the future [11].

Fifth, some organizations disclosed that they were working and cooperating with law enforcement on the incident [12].

Not all corporations that disclosed an information security breach followed the steps above. In the Bank of America / Wachovia case, Commerce Bank and PNC Bank of Pittsburgh were also affected. Commerce Bank did not return phone calls to those seeking comments and PNC would not disclose how many of their customers were effected [10]. In this case, these smaller banks were overshadowed by the larger institutions. If it is only you in the spotlight, you will most likely need to respond with more information.

To conclude:

Incidents are like bad weather: we do not have control over them but we can properly prepare ourselves and have the proper reaction should something happen. We need to have the correct foundations to weather the storm. But sometimes a violent storm occurs: people realize this as a risk for living in a particular region.

Similarly, by doing due diligence we can prepare a strong foundation. If you do the right thing, people understand that the road is bumpy and that not everything goes gracefully. There is an inherent risk to using information systems and some circumstances are not within our control: they are in the hands of others or chance. Public trust is important to maintain.

The take away points are as follows:

* Protect your core business functions/systems as well as your non-core functions / systems.
* Do due diligence – protect your information systems to a reasonable degree.
* Should an incident occur, react properly.

And, let the chips fall where they may because:

It is difficult to ruin one's reputation.

Thank you.

Conference Attendee Responses:

1. Some companies were proactive in their response. For example, Discover Card issued new cards after the DSW Shoe Warehouse breach. These proactive actions were not taken into account.

2. Reputational Risk still seems unquantifiable. True costs associated with a security breach are buried. It will not be until it becomes a line item on the annual report that we truly understand the impact of a breach.

3. There was an ethical component to the Arthur Anderson case that does not appear to be present in the other security breaches.

4. People do not understand what it means to have their data compromised. We see there are reports of the breach, but we do not see follow-up reports. It is only when the public sees the impact to individuals will reputational damage increase. (For example, only after we hear of stories of little old ladies losing their life savings because of a security incident will the public begin to understand the impact of a breach.)

5. My paper tends to focus on consumer behavior. Institutions may be major shareholders of some stocks mentioned. They may be less inclined to sell the equity due to a breach. That is why we do not see a significant decrease in price.

My replies:

1. True. This was not taken into account.

2. While it is still difficult to quantify because of many factors, perhaps the stock price may give some indication although it is clearly not perfect. I also mention in the paper that one limitation to my research is that I do not have internal corporate data which may give a fuller or different picture. Further, certain cross-institution statistics such as accounts closing at one institution and opening at another just seem impossible to acquire without a prior agreement between institutions.

3. True. My only point with the Arthur Anderson case is that the conflict of interest effected their core business just as the breaches did in the cases of CardSystems and Choicepoint.

4. True. I believe the landscape regarding information security breaches and reputational risk will change over time due to 1) varying types of breaches 2) number of reported breaches 2a)in general and 2b) per specific institution.

5. True. I think this supports me, though. It seems to me that institutional investors will look at the financial impact more than the individual investor.

Biography of Kenneth F. Belva:

Kenneth F. Belva is currently employed at Credit Industriel et Commercial (New York) as their Information Security officer where he reports directly to the Senior Vice President and Deputy General Manager. He is currently on the Board of Directors for the New York Metro Chapter of the Information Systems Security Association. He has presented on topics such a patch management as well as moderated a panel discussion on corporate governance. He taught as an Adjunct Professor in the Business Computer Systems Department at the State University of New York at Farmingdale. Mr. Belva is credited by Microsoft and IBM for discovering vulnerabilities in their software. He is the author of the chapter "Encryption in XML" in *Hackproofing XML* published by Syngress. Mr. Belva holds the Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) certifications and has passed the Certified Information Security Manager (CISM) exam.

*** Mr. Belva would like to thank Sam H. DeKay for the recommendation to speak at the FiTech Summit where this paper was delivered. He would also like to thank Patrick Leahy for the Bloomberg charts, his good spirits and his market wisdom.

References:

[1] Bank security breach may be biggest yet
http://money.cnn.com/2005/05/23/news/fortune500/bank_info/

[2] Citigroup Blames UPS For Customer Data Loss
http://www.forbes.com/facesinthenews/2005/06/06/0606autofacescan09.html

[3] Citigroup, Bank of America on deck
http://www.marketwatch.com/news/yhoo/story.asp?source=blq/yhoo&siteid=yhoo&dist=yhoo&guid=%7B9F9338F5%2D5D08%2D4BB9%2D8921%2D6821ADA2FAA3%7D

[4] BofA, Wachovia named in lawsuit
http://biz.yahoo.com/bizj/050623/1123999.html?.v=1

[5] MasterCard: 40M Credit Card Accounts Exposed
http://www.internetnews.com/security/article.php/3513866

[6] ChoicePoint to Exit Non-FCRA, Consumer-Sensitive Data Markets; Shift Business Focus to Areas Directly Benefiting Society and Consumers
http://www.choicepoint.net/85256B350053E646/0/61E8CEB66AAA285485256FBA00413724?Open

[7] Visa cuts CardSystems over security breach
http://www.theregister.co.uk/2005/07/19/cardsystems/

[8] Wendy's 2Q Sales Hurt by Finger Hoax
http://biz.yahoo.com/ap/050707/wendy_s_sales.html?.v=7

[9] The CardSystems blame game
http://www.securityfocus.com/print/columnists/344

[10] Banks Notify Customers of Data Theft
http://abcnews.go.com/Business/wireStory?id=783320

[11] U.S.: CitiFinancial Statement on Lost Data Tapes
http://www.citigroup.com/citigroup/press/2005/050602e.htm

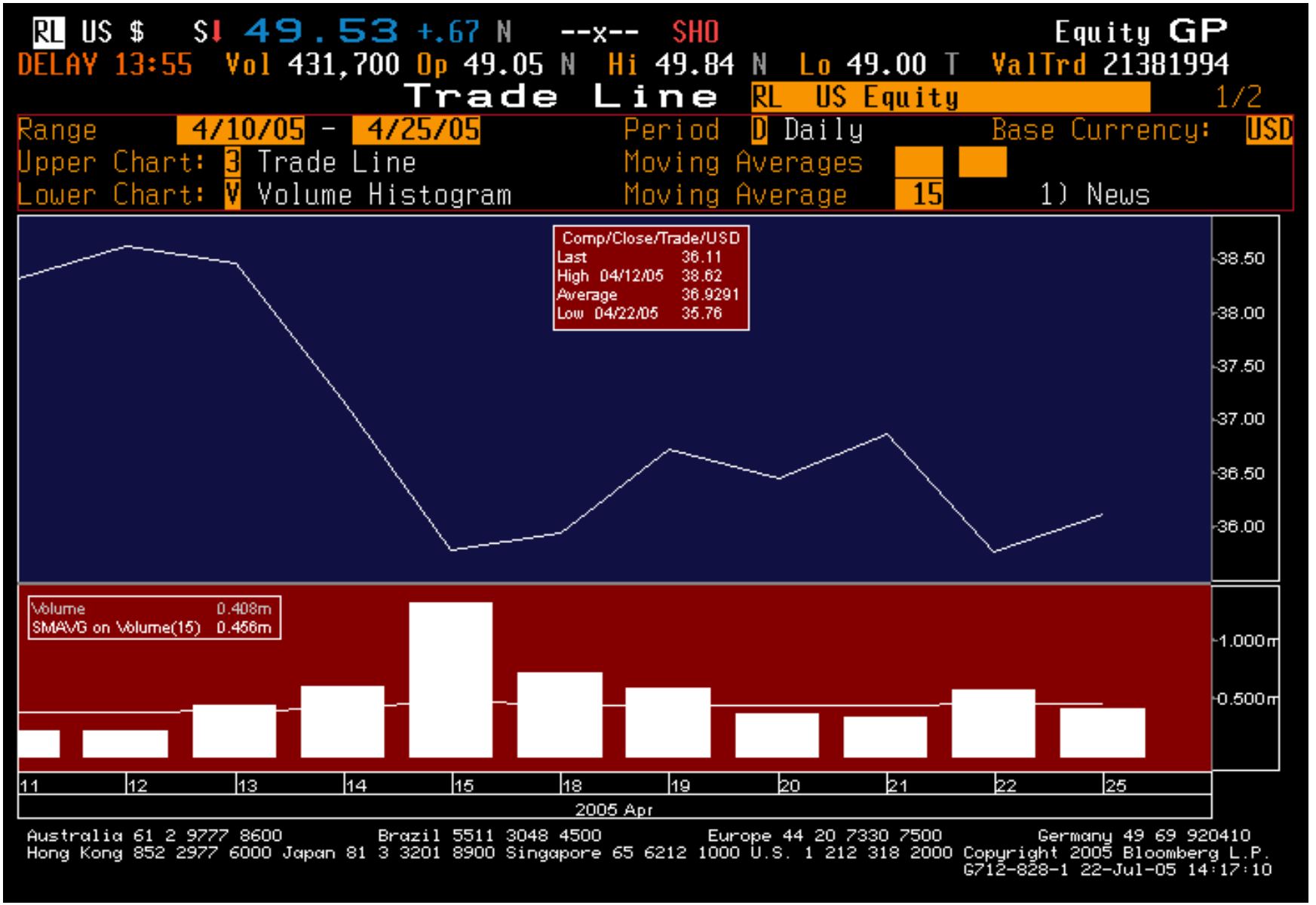
[12] Statement on Lost Data Tapes – Employee Letter
http://www.timewarner.com/corp/newsroom/employee_data_tapes/employee_letter.html

[13] Statement on Lost Data Tapes – Q & A
http://www.timewarner.com/corp/newsroom/employee_data_tapes/faq.html

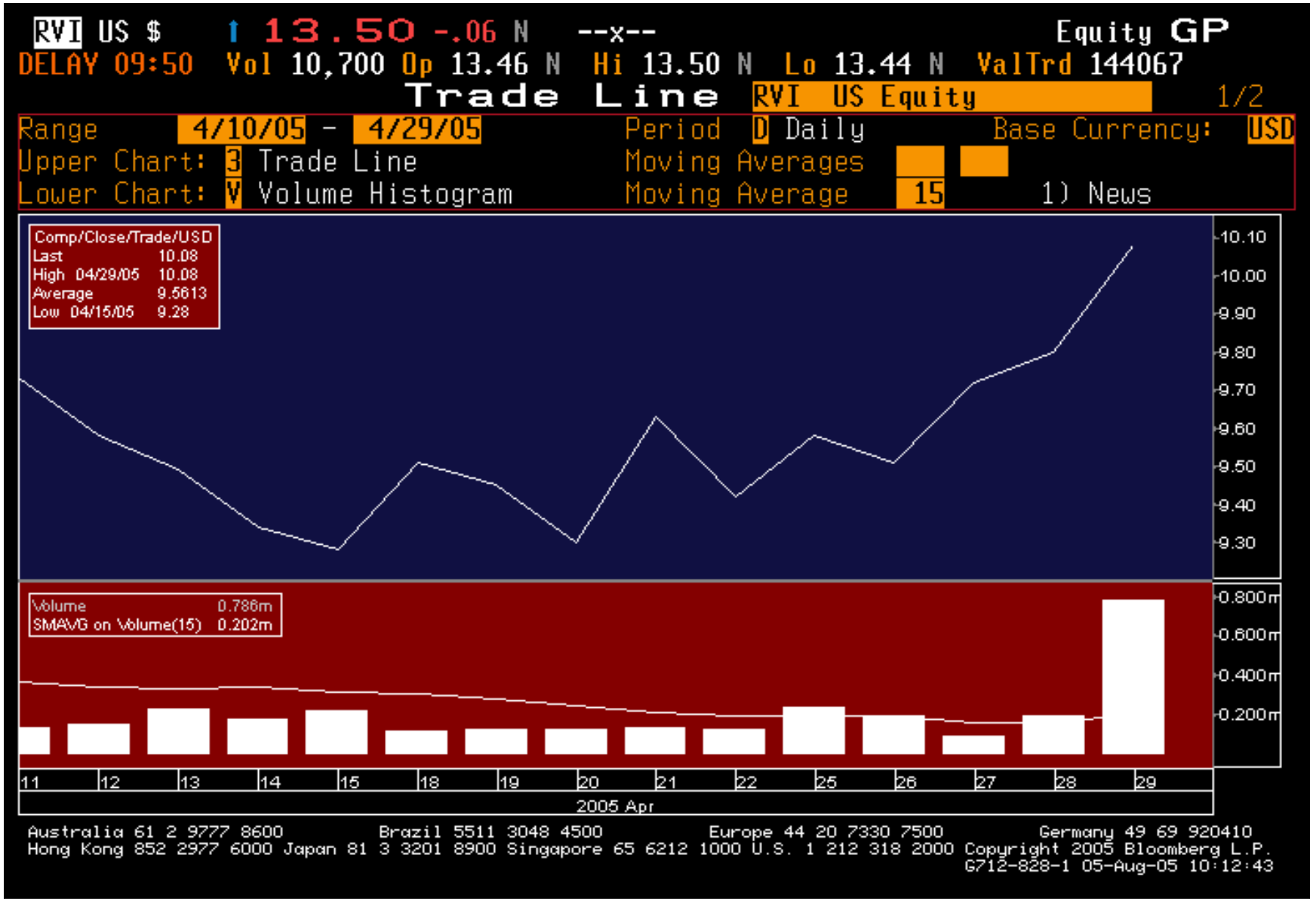
[14] Polo Ralph Lauren Customers' Data Stolen
http://sfgate.com/cgi-bin/article.cgi?f=/n/a/2005/04/14/financial/f064639D31.DTL

[15] (DSW Press release on stolen information)
http://www.dswshoe.com/ccpressrelease/pr/ (March)
http://www.dswshoe.com/ccpressrelease/pr/CCAprilUpdate.html (April)
http://www.dswshoe.com/credit_card_faq.jsp (April)

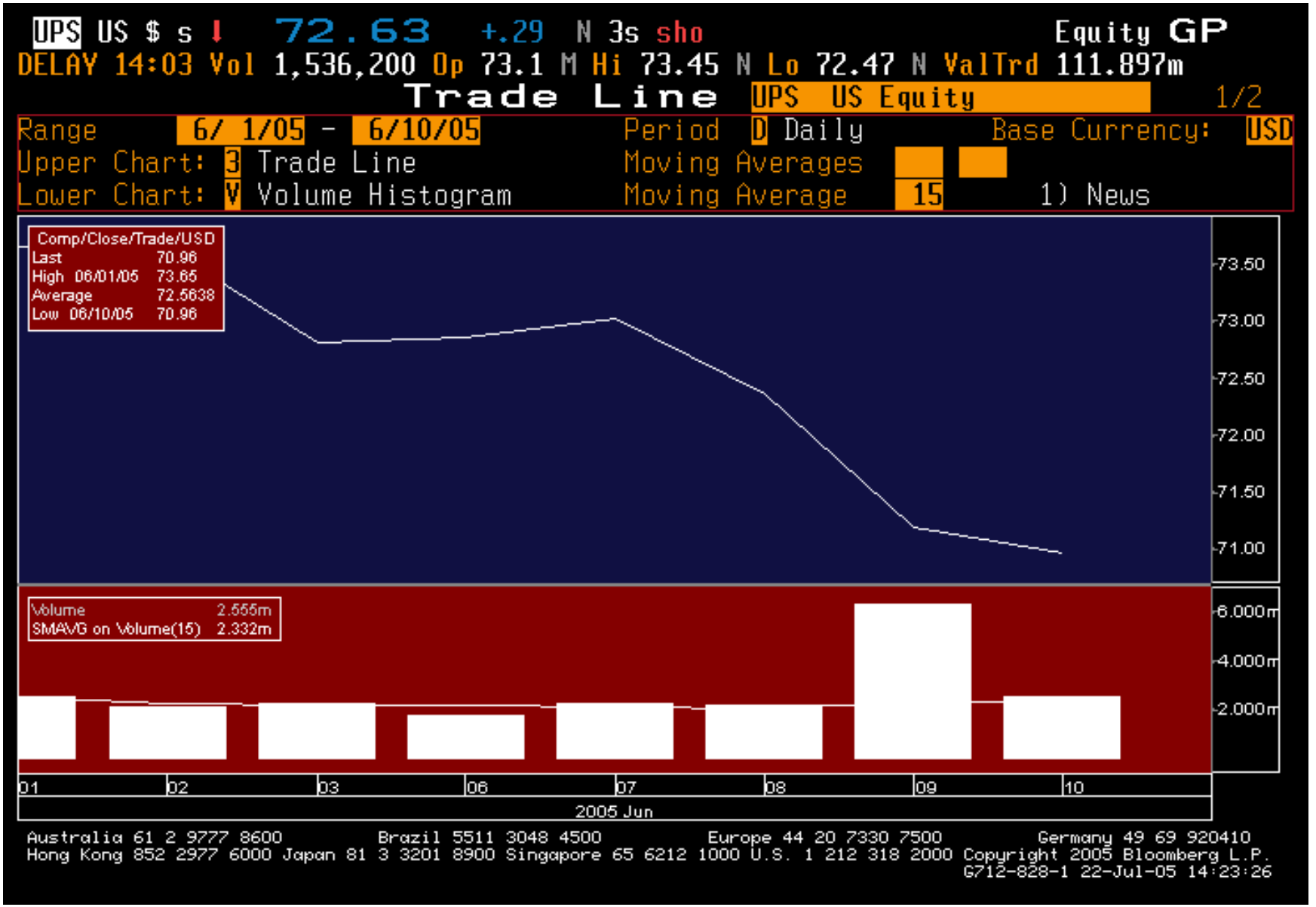
Polo Ralph Lauren - Specific



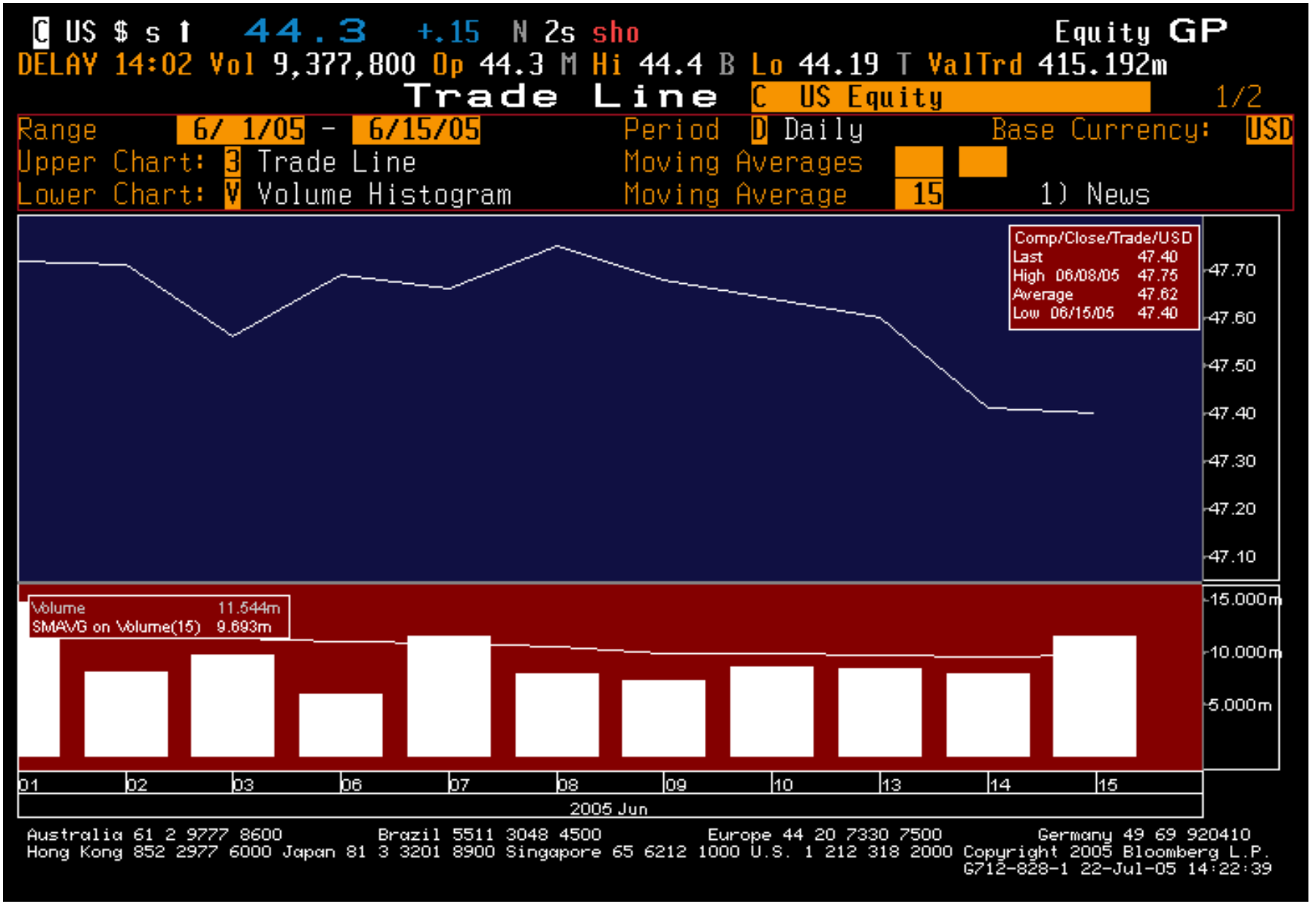
DWS Show Warehouse (Retail Ventures Inc.) - Specific



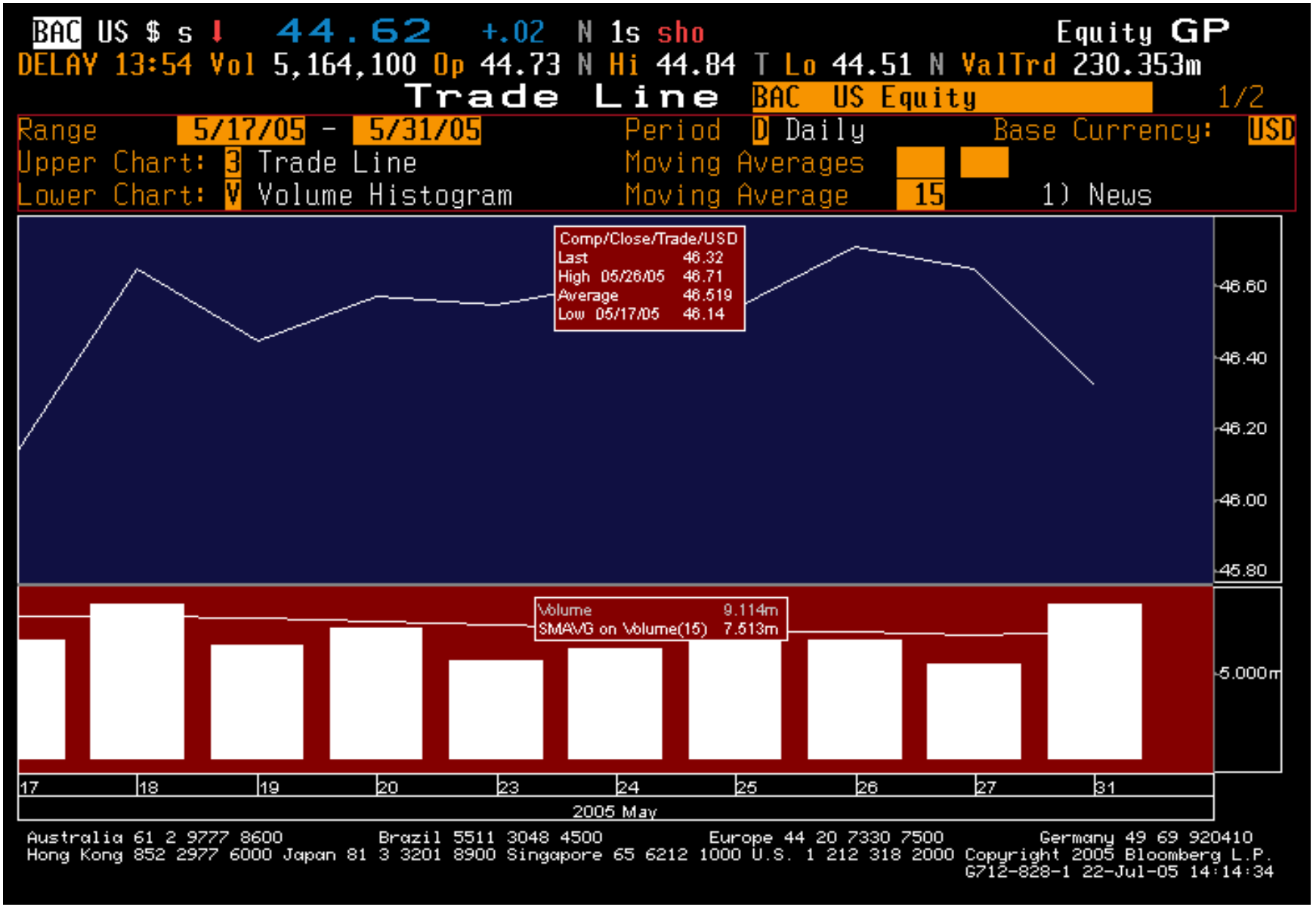
UPS - Specific



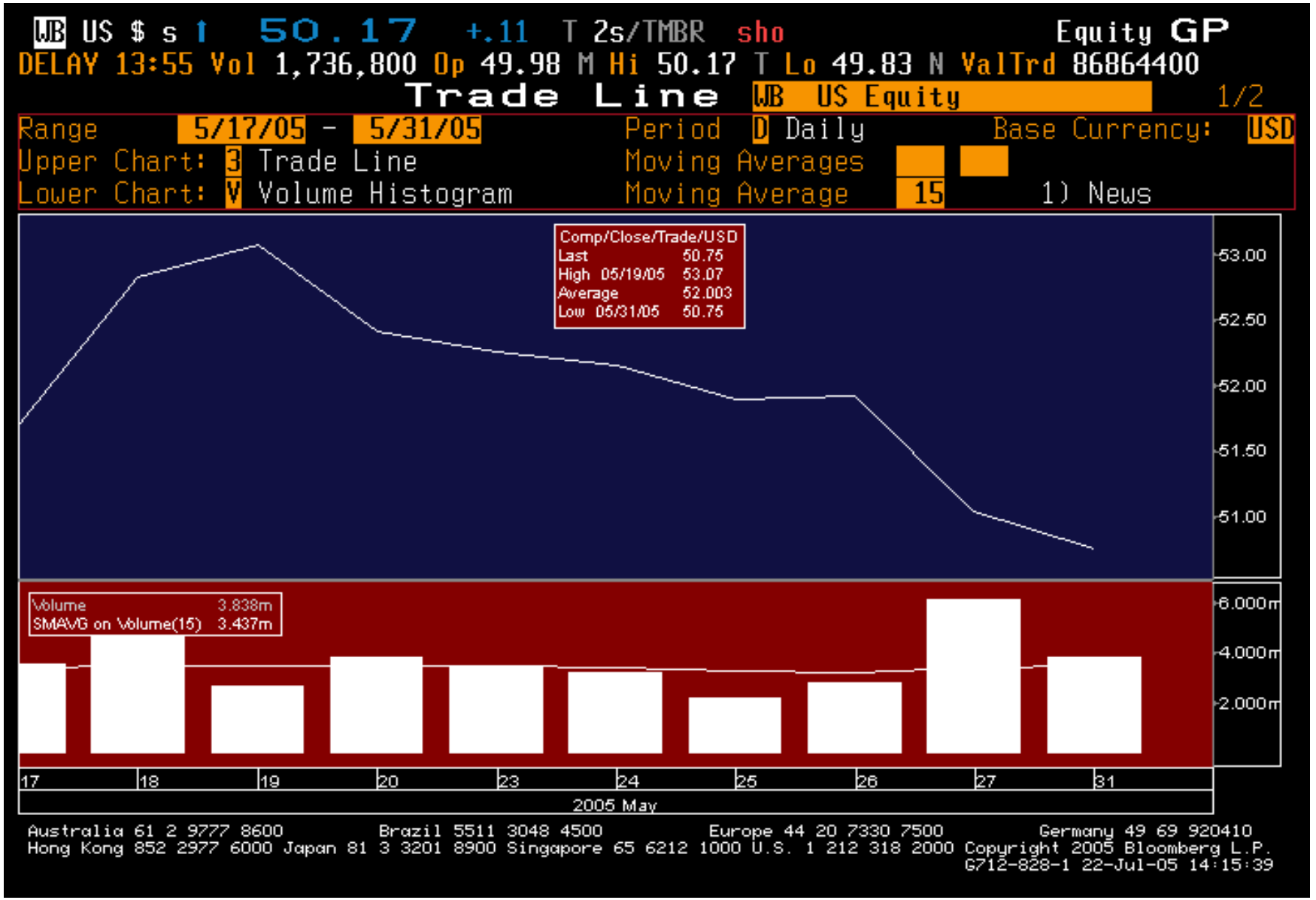
Citigroup - Specific



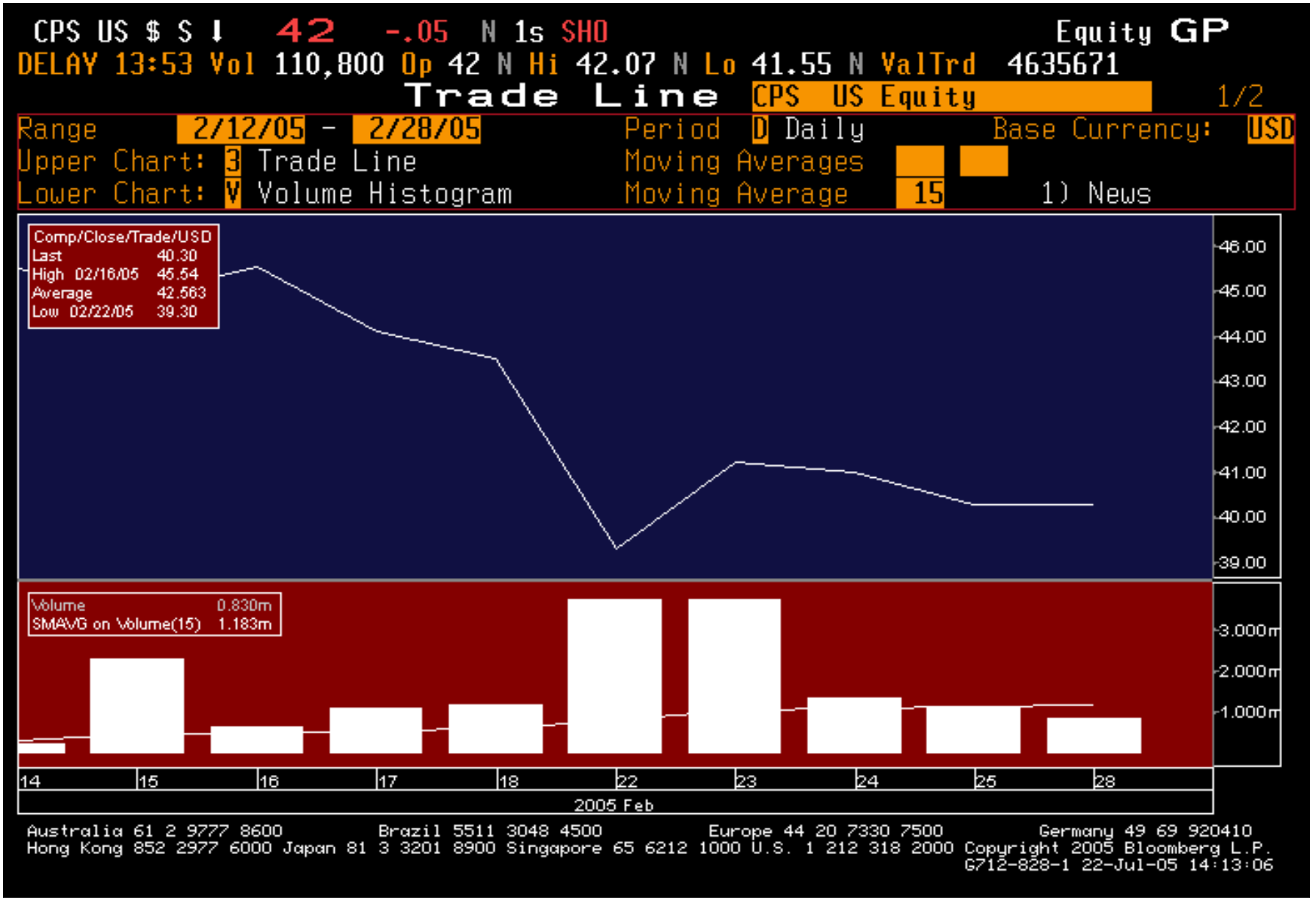
Bank of America - Specific



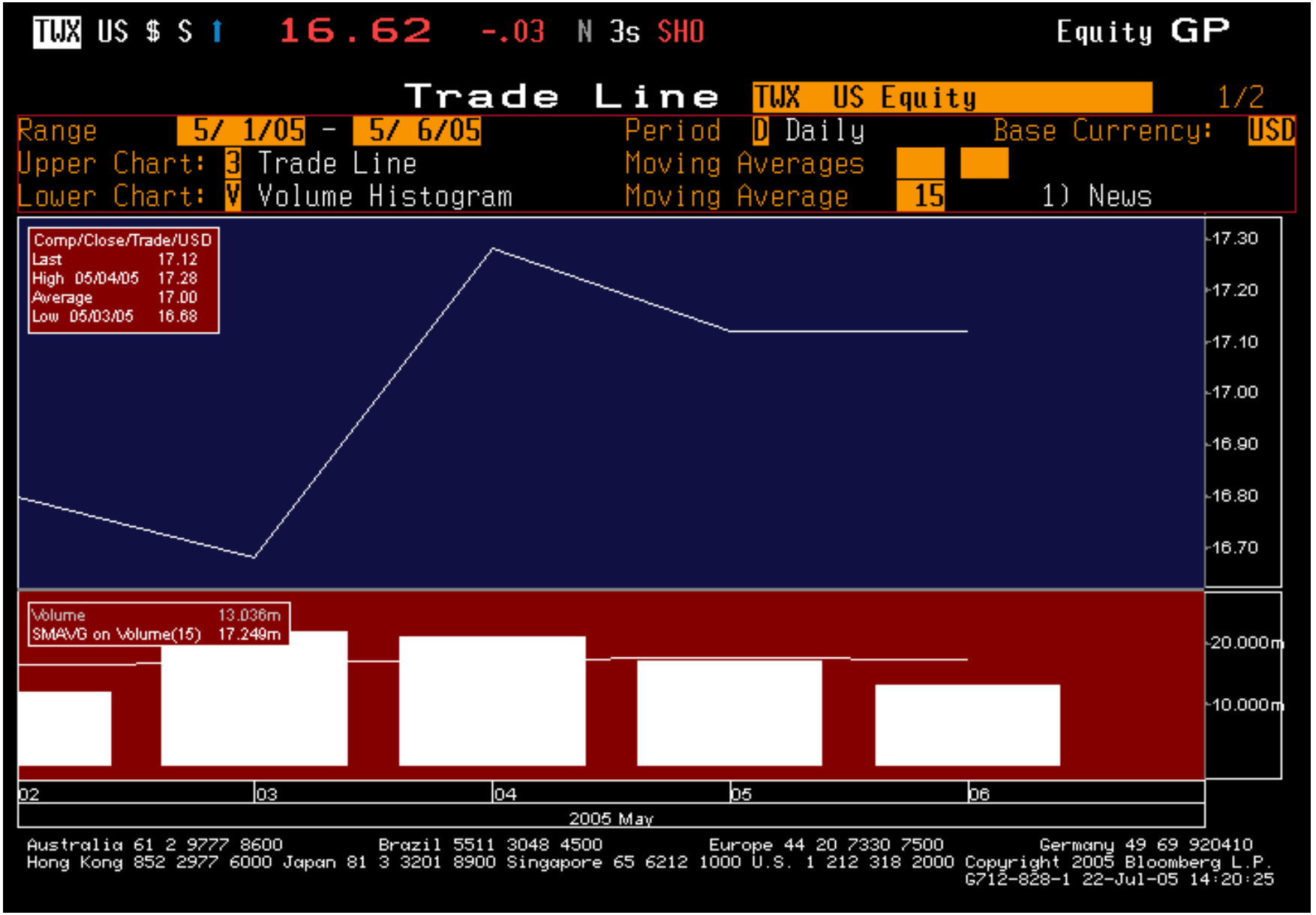
Wachovia - Specific



Choice Point - Specific



Time Warner - Specific



Polo Ralph Lauren - Trend

DWS Show Warehouse (Retail Ventures Inc.) - Trend

Citigroup - Trend

Bank of America - Trend

Wachovia - Trend

Choice Point - Trend

UPS - Trend


UPS US $ st 72.76 +.42 N --x-- sho
Equity GP
DELAY 12:26 Vol 1,218,900 Op 73.10 M Hi 73.45 N Lo 72.47 N ValTrd 88854744
Trade Line
UPS US Equity
1/2
Range 6/ 5/05 - 7/22/05
Period D Daily
Base Currency: USD
Upper Chart: 3 Trade Line
Moving Averages
Lower Chart: V Volume Histogram
Moving Average 15
1) News
Comp/Close/Trade/USD
Last 72.76
High 06/07/05 73.02
Average 70.3112
Low 07/06/05 67.71
73.00
72.00
71.00
70.00
69.00
68.00
Volume 1.219m
SMAVG on Volume(15) 2.813m
5.000m
06 07 08 09 10 13 14 15 16 17 20 21 22 23 24 27 28 29 30 01 05 06 07 08 11 12 13 14 15 18 19 20 21 22
2005 Jun
2005 Jul
Australia 61 2 9777 8600 Brazil 5511 3048 4500 Europe 44 20 7330 7500 Germany 49 69 920410
Hong Kong 852 2977 6000 Japan 81 3 3201 8900 Singapore 65 6212 1000 U.S. 1 212 318 2000 Copyright 2005 Bloomberg L.P.
G712-828-1 22-Jul-05 12:46:30

Time Warner - Trend