Testimony of
Joseph Ansanelli
Chairman and CEO of Vontu, Inc.

June 24, 2003
2128 Rayburn House Office Building
Washington, D.C.

Before the United States House of Representatives
Subcommittee on Financial Institutions and Consumer Credit
"Fighting Identity Theft – The Role of FCRA"

Introduction

My name is Joseph Ansanelli and I am the CEO and founder of Vontu. We provide information security software that guards against the loss of customer information. I am honored to provide testimony on fighting identity theft and the role of the Fair Credit Reporting Act. And I commend the Subcommittee members for discussing this important issue.

My testimony draws from my experience in working with Chief Information Security Officers at some of the country's top financial services, insurance, media and retail companies. These security professionals are acutely aware of the challenges in adequately protecting consumer information.

The Insider Security Threat

To begin, we believe it is important to help a consumer quickly repair his or her credit when their identity has been stolen. However, the problem will continue to grow if we do not prevent the theft of consumer data in the first place. While there are many ways identity theft occurs –a financial report stolen from the trash, a credit card receipt in a restaurant - companies and government agencies are the ultimate sources for large electronic databases

of consumer information. Without additional safeguards in place, millions of Americans may be victims of identity theft by the end of this decade.

Traditionally, organizations have focused on the "hacker" and preventing break-ins to their customer data systems. Many organizations now realize that another significant threat exists. With the rapid adoption of the Internet and tools such as electronic mail, consumer information can be leaked in a moments notice by insiders. No matter how secure an organization's systems are, they must maintain many employees' access to sensitive customer data. Yet, it is much easier for employees to accidentally leak or maliciously steal information than it is for a thief to break in from the outside.

For example, in November 2002, a customer service employee of Teledata Communications Inc. who had easy access to consumer credit reports allegedly stole 30,000 customer records. This theft caused millions of dollars in financial losses and demonstrates that even though any computer system can be hacked, it is much easier, and in many cases far more damaging, for information to be stolen from the inside.

In May 2003, we conducted a survey with Harris Interactive of five hundred employees and managers with access to customer data. Almost half of the workers and managers said it would be "easy" to take sensitive customer information from their employers' network. Two-thirds believed their co-workers posed the greatest risk to consumer data security. Only ten percent said hackers were the biggest risk. It is important to look beyond external threats and recognize that insiders pose a fast growing risk.

Fighting Identity Theft and the Role of the Fair Credit Reporting Act

Based on my experience, I recommend the Subcommittee weigh the following when considering revisions to the Fair Credit Reporting Act.

Confusion is the Enemy of Consumer Protection

First, confusion is the enemy of consumer protection. A consistent and unified national approach to our credit system will benefit consumers the most. However well-intentioned a system of fifty different laws might be, it would only create confusion and paralysis that would ultimately harm consumer protection. Therefore, we believe that the preemption

provisions of the Fair Credit Reporting Act are critical and should extend to any additions to help protect against identity theft.

"Safe Harbor" for Best Practices

Second, we urge the Subcommittee to ensure that any modifications to the Fair Credit Reporting Act encourage companies to go above and beyond any stated requirements to protect consumers. Most companies know it is in their self interest to protect a customer's data. However, I have had companies question whether they should go beyond base legislative and regulatory requirements for fear in doing so could potentially reveal problems that trigger punitive actions. Future legislation should encourage and protect organizations that go beyond any base security requirements.

Consumer Data Security Standard

Third, I suggest this committee develop a Consumer Data Security standard as part of the Fair Credit Reporting Act. Ensuring a national, unified and standard approach to protecting consumer information will help to stop one of the main and growing sources of identity theft. Any such standard should include the following principles:

1. First, corporate security policies should be mandated. A company's security policies should be publicly available, regularly reviewed and updated, and audited and approved by its Board of Directors.

2. Second, employee education is critical. In the Harris survey I referenced earlier, almost one-third of workers and managers had not read or did not know if their company had a written consumer data security policy.

3. Third, data protection and control should require best practices. Physical and network protection should use best practices though all commercially reasonable solutions.

4. Fourth, companies must enforce employee compliance. Organizations should have an obligation to regularly monitor and enforce employee compliance with government regulations and internal security policies for the use and distribution of sensitive consumer information.

I hope these comments will prove helpful to the subcommittee as it continues its deliberations on the Fair Credit Reporting Act. I welcome the opportunity to continue working with you and am happy to answer any questions you might have.

Joseph Ansanelli
Chairman and Chief Executive Officer
Vontu, Inc.
(415) 227-8100

Consumer Data Security Survey Highlights

The following questions and responses are highlights of a survey of 500 U.S. workers and managers that handle sensitive customer information at work. The data for the survey was collected in May 2003 by Harris Interactive Service Bureau (HISB) and analyzed by Vontu.* Only workers and managers who said they have access to customer information were qualified to complete the survey.

- 62% reported incidents at work that could put customer data at risk for identity theft
- 66% say their co-workers, not hackers, pose the greatest risk to consumer privacy. Only 10% said hackers were the greatest threat.
- 70% say that government regulations play a role in raising awareness at their workplace about identity theft and database security
- Nearly 50% say government has still not done enough to help thwart identity theft.
- 46% say it would be "easy" to "extremely easy" for workers to remove sensitive data from the corporate database.
- 32%, about one in three, are unaware of internal company policies to protect customer data

Some of the more compelling questions and answers from the survey follow:

Does your company have a policy regulating what information is not okay to send out through email, Web mail, IM, etc.?

Yes 68.16%
No 14.56%
Not sure 17.26%

Have you read this policy in its entirety?

Yes 79.77%
No 20.23%

How would you characterize the level of security protecting customer information on your company's network?

Not at all secure 1.75%

Not very secure 5.44%

Somewhat secure 12.82%

Secure 19.61%

© Copyright 2003 Vontu, Inc. All Rights Reserved.

Very secure **27.77%**

Extremely secure **26.41%**

Not sure **6.21%**

How easy would it be for someone at work to remove sensitive customer data from the corporate network?

Extremely difficult **10.87%**

Very difficult **11.07%**

Difficult **17.28%**

Easy **25.44%**

Very easy **11.07%**

Extremely easy **8.54%**

Not sure **15.73%**

Which do you think poses the greatest threat to customer privacy and database security at your workplace?

Hackers who break into the network **10.49%**

Workers at the company who abuse their access privileges **18.06%**

Workers who have legitimate access to customer data **26.02%**

A lack of understanding or education among workers **22.14%**

I don`t think there is any threat to customer privacy and data **23.30%**

How do you access sensitive information that might include Social Security numbers, credit card numbers, account numbers or passwords? ***Please select all that apply****.*

Web-based application **19.68%**

Database application **62.76%**

Documents **66.13%**

Printouts **41.22%**

Other **14.57%**

Please indicate if you are aware of the following regulations.

© Copyright 2003 Vontu, Inc. All Rights Reserved.

- Gramm-Leach-Bliley Act or GLBA

  Yes 15.34%

  No 84.66%

- California SB1386

  Yes 5.24%

  No 94.76%

Now we'd like to ask some questions about your views on how involved the U.S. federal government should be in workplace issues.

Do you believe that government regulations encourage workers with access to sensitive information to be more aware of protecting that data?

Yes 67.83%

No 32.17%

Do current privacy regulations and policies help or hinder your efforts to protect sensitive information?

Help 35.38%

Hinder 10.22%

Neither 54.40%

On a scale of 1 to 5 with 1 not being enough and 5 being too much, please tell us if you believe the government has done enough to protect identity theft and customer data.

1	**Government has not done enough**	**25.02%**
2		**25.22%**
3		**34.70%**
4		**8.93%**
5	**Government has done too much**	**6.13%**

***** *Data for this survey were collected by the Harris Interactive Service Bureau (HISB) on behalf of Vontu. HISB was solely responsible for the quality of the online data collected and did not perform the survey design, data weighting or data analysis.*

© Copyright 2003 Vontu, Inc. All Rights Reserved.