

# Information Exposure: A Critical Need for Expertise

---

*A Case Study by: Dr. John White*

Author:

*Dr. John White*

*Criminal Justice Program Coordinator, Professor*

*Martin Methodist College*

January 2011

*Information Exposure: A Critical Need for Expertise*

Copyright © 2011 Dr. John White

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owners.

**DISCLAIMER:**

The foregoing is not and is not intended as legal advice, or the author purporting to be qualified legal counsel. Legal questions should be referred to professionally licensed legal counselors within the jurisdiction of the issued raised.

Published by Dr. John White, January 2011

Any comments relating to the material contained in this document may be submitted to:

Martin Methodist College  
Department of Criminal Justice  
433 West Madison Street  
Pulaski, TN 38478  
931-424-7375

or by email to:

[jwhite@martinmethodist.edu](mailto:jwhite@martinmethodist.edu)

## **Table of Contents**

---

<b>Executive Summary</b>	<b>4</b>
<b>Have we done what is necessary?</b>	<b>5</b>
<b>Our Efforts Left Us Exposed</b>	<b>6</b>
<b>Choosing the Right Expert Makes a Difference</b>	<b>7</b>
<b>Day One: Behavioral, Operational, and Technological Assessment</b>	<b>8</b>
<b>Day Two: Putting the Pieces Together</b>	<b>9</b>
<b>Conclusion</b>	<b>10</b>
<b>About the Author</b>	<b>11</b>

*The scope of information exposure has become so broad that executives are encouraged to bring in industry experts to manage their risk.*

## **Executive Summary**

---

The information compliance and prevention environment has never been more intense. Over 500 million personal records have been lost or stolen from businesses, schools, government agencies, and other organizations within the past five years. Executives in entities of every size are discovering that they are not only unprepared to assess the full scope of risks and legal requirements, but that they are also left with *personal liability* for the shortfalls of their Identity Theft Prevention Programs.

Dr. John White, the Criminal Justice Program Coordinator at Martin Methodist College, shares his experience before and *after* bringing in an expert to limit the institutions information exposure. He cautions executives and administrators not to shortcut their compliance and prevention efforts.

## Have we done what is necessary?

Recently, I wrote a white paper discussing vicarious liability as it relates to information management issues in the workplace. Having personally participated in liability cases, I have followed these issues very closely.

*“When considering the approach adopted by the Federal Trade Commission’s (FTC) Red Flags Rule it would be prudent for administrators and policymakers to bear in mind that the level of personal responsibility they carry is one of serious import for them as individual persons because of a legal concept commonly known as, vicarious liability. (The Information Age of Vicarious Liability)”*

*“It forced me to ask some serious questions about my own organization.”*

Writing this piece caused me to think about Martin Methodist College where I am currently a professor and the Criminal Justice Program Coordinator. It forced me to ask some serious questions about my own organization.

- ◆ Do we have adequate policies and procedures in place for the protection of personal information?
- ◆ Have we done an exhaustive risk assessment to expose our liabilities?
- ◆ Did we employ the right expertise to limit the vicarious (personal) liability of our college, Board members, executives, administrators, and faculty?
- ◆ What measures do we currently have in place to detect, prevent, and mitigate losses or breaches of information?
- ◆ How would we fare in an information security incident?

## Our Efforts Left Us Exposed

Becoming concerned, I began asking questions in departments such as public safety, information technology, human resources, and finance. What I found surprised me. There were some policies and procedures in place. However, while we have experts in each of these areas, none of our staff had expertise specific to identity theft prevention and bringing our *complete* information exposure into scope. Our current assessment and training did not translate into actions required by law to detect, prevent, and mitigate identity theft. I was concerned that there would be gaps in our compliance and prevention efforts leaving myself and others in our college potentially liable in the event of a breach.

*” Our current assessment and training did not translate into actions required by law to detect, prevent, and mitigate identity theft.”*

*“The Trier of fact might determine such sources were insufficient to establish a reasonable basis of executive knowledge and still hold the manager liable for what he or she “should have known”. Relying upon non-specialist, or limited skilled personnel, to assess complex management issues brings future tort liability to the level of a simple gamble. (The Information Age of Vicarious Liability)”*

After discussing my findings with the executive staff our course became clear. In order for Martin Methodist College to create an Identity Theft Prevention Program that would constitute a “reasonable effort” in a court of law, we would have to partner with an industry expert. The experts would have to be field-trained with practical experience assessing information exposure at an enterprise level for higher education. Just as important they would have to facilitate custom solutions for any compliance and prevention concerns. In other words, no “cookie cutter” assessments and punch lists.

*“In order for Martin Methodist College to create an Identity Theft Prevention Program that would constitute a “reasonable effort” in a court of law, we would have to partner with an industry expert.”*

*“[i]n certain areas of the law recklessness is considered a form of intentional conduct for purposes of imposing liability for some act.” Recklessness means that the manager, even if they made efforts to assess the management environment, was not diligent enough in their assessments. (The Information Age of Vicarious Liability)”*

Through our due diligence process the college interviewed certified public accountants, attorneys, and information technology specialists. Each demonstrated expertise in areas of information security specific to their profession. We also looked at “one-stop-shops” that proclaim to do everything, but do not specialize in any one area. However, with so much at stake, we were really looking for a specialist that could help us identify and mitigate our risk for information loss or breach. This is an enterprise risk management issue.

## Choosing the Right Expert Makes a Difference

*“The consultant expressed an in-depth understanding of information legislation and prevention issues.”*

*“We hired Identity Theft Loss Prevention, LLC to assess our current “program” and to facilitate solutions to reduce liability.”*

One afternoon, I was introduced to Identity Theft Loss Prevention, LLC on a FACT Act Red Flags Rule compliance webinar. The consultant expressed an in-depth understanding of information legislation and prevention issues. He confidently exuded practical experience with incorporating all of these moving parts into a comprehensive Identity Theft Prevention Program for higher education.

*“To accomplish this, managers would be well advised to make every effort reasonably available to them to familiarize themselves with all aspects of each issue from which a tort action might arise. This requires not only the investment of time and research but the expertise relevant to the issue at hand. (The Information Age of Vicarious Liability)*

We hired Identity Theft Loss Prevention, LLC to assess our current “program” and to facilitate solutions to reduce liability. The following is an account of our experience with the *information* Compliance and Awareness Process. Martin Methodist College has never experienced risk management like this.

## **Day One: Behavioral, Operational, and Technological Assessment**

*“The Identity Theft Loss Prevention consultant found over 150 areas of concern.”*

*“We learned that current widely accepted practices for detecting and preventing information loss in higher education institutions does not address the methods used by thieves today, which is probably why education has become their number one target over the past five years.”*

The first day of engagement began with a *college-wide* identity theft assessment. Our business and administrative departments were assessed. The department heads were interviewed. Specific operational and technological concerns were cited. The Identity Theft Loss Prevention consultant found over 150 areas of concern. Some were obvious issues, while others took more digging to have them surface. We realized that internally we did not know the full extent of what to ask and or where to look. Using an outside experts gave us the necessary third-party perspective to bring our liability into scope.

Unbeknownst to our highly trained and well-intentioned staff, confidential and sensitive information was easily accessed by these “thieves for hire.” We learned that current widely accepted practices for detecting and preventing information loss in higher education institutions does not address the methods used by thieves today, which is probably why education has become their number one target over the past five years. The fact is, as deeply rooted in all of academic culture, our employees, faculty, and students were unconsciously willing to give out information that could result in a major breach. In fact, if this had not been an assessment exercise, our college staff and board members would have found themselves in dire straits and the stability of our college would be in serious trouble.

## Day Two: Putting the Pieces Together

*“In just hours each department had identified their covered accounts, patterns of red flag activity, and appropriate responses for each employee!”*

*“The tangible results of these working sessions yielded custom policies, procedures, training, structure, and an implementation strategy with feasible practical steps.”*

On the second day, Identity Theft Loss Prevention consultants collaborated with our department heads to uncover information usage issues addressed by the FACT Act Red Flags Rule. In just hours each department had identified their covered accounts, patterns of red flag activity, and appropriate responses for each employee! Furthermore, there was a buzz going around campus about the social engineering activity. Our relaxed culture was quickly becoming aware of the seriousness of the information in our care.

After the department head meeting, our Identity Theft Prevention Team came together to work with the specialists through the *information* Compliance and Awareness Process. We discussed the findings of the audits and the social engineering. As a group we delved deeper into our information management processes to expose new vulnerabilities. The tangible results of these working sessions yielded custom policies, procedures, training, structure, and an implementation strategy with feasible practical steps. The steps would be reasonable to implement as all of our Team collaborated on these working solutions with the specialists.

The intrinsic results were the most impressive. Due to the combination of social engineering, assessments, and other steps that Identity Theft Loss Prevention took, employees were asking questions of themselves. They realized that a breach could happen here. A change of culture had started to take place. Suddenly, policies and procedures were becoming less of a hassle and more a necessity. All staff seemed to recognize how important following protocol is, in order to ensure a safe environment for all Confidential and Sensitive Information that we handle daily and store for future use.

Finally, our consultants addressed our executive staff with a tactfully presented, high-level overview of the assessments, our risk exposure, and the collaborative effort currently underway to mitigate these concerns. Due to the professional presentation, our Identity Theft Prevention Team on campus gained much needed support for the Identity Theft Prevention Program and serious attention to requests for resources. Sometimes a third-party expert can say the things that need to be said because they are outside of the organization's internal politics.

## Conclusion

*“Your people can only test what they know. However, a third-party expert can expose what you should have known.”*

As information becomes more valuable to establish identities for commerce, the liability for higher education institutions and the vicarious liability for those employed there is now a key focus for risk managers. In order to mitigate these dynamic and changing issues, policy makers are strongly encouraged not only to collaborate with peers on campus, but to engage the expertise of identity theft professionals. Your people can *only* test what they know. However, a third-party expert can expose “what you should have known.” Based on our experience, I would strongly suggest Identity Theft Loss Prevention, LLC. The cost savings between doing-it-yourself and working with an expert could be your own . . . *vicarious liability*

## About the Author

Dr. John White is a professor and the Criminal Justice Program Coordinator at Martin Methodist College in Pulaski, Tennessee.

### **Education:**

BS: Law Enforcement; University of North Alabama

MCJ: Criminal Justice; Middle Tennessee State University

Ph. D.: Public Administration; Tennessee State University

### **Professional Experience:**

1969 – 1972: Reserve Police Officer Vallejo Police Department, Vallejo, CA

1971: Deputy Sheriff, Alameda County Sheriff's Dept. Oakland, CA

1972 – 2000: Police Officer Pulaski Police Dept. Pulaski, TN

1987 – 1991: Governor's appointment, board member Tennessee Peace Officer's Standard and Training Commission

1986 - Co-founder and past President; Tennessee Law Enforcement Training Officers Association

### **Public Service:**

1999 – 2003: Giles County Commission; dist. 7

2000 - 2003: Chairman of the Giles County Commission

### **Teaching Experience:**

Cumberland University; undergraduate and graduate schools

Athens State University

Martin Methodist College

Columbia State Community College

Tennessee Law Enforcement Training Academy

Special guest lecturer various training schools and sessions

Program Coordinator Criminal Justice degree Martin Methodist College

Director of Security Martin Methodist College

### **Courtroom Experience:**

1971 – 2009: Testified in local, state and federal courts in both criminal and civil cases

1985 – 2000: Participated in several liability suits in federal court