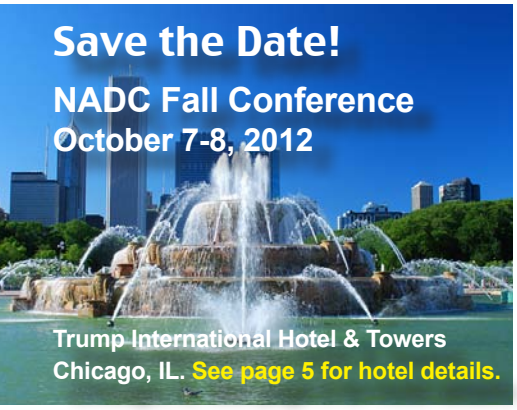
NADC
National Association of Dealer Counsel

# DEFENDER

The National Association of Dealer Counsel Newsletter JUNE 2012

In this Issue:






Contact Us:

NADC
1155 15th Street, NW
Suite 500
Washington, DC 20005
Phone: 202-293-1454
Fax: 202-530-0659
www.dealercounsel.com

## EEOC Holds That Transgender Workers Are Protected by Title VII

*By Jerry Stovall, Breazeale, Sachse & Wilson, L.L.P.*

The Equal Employment Opportunity Commission continues to make news with its rulings and its rules. In April, the EEOC issued one of each, both of which many on both sides of the fence are calling "groundbreaking". First, the EEOC ruled that a complaint of discrimination based on **gender identity, change of sex, and/or transgender status** is cognizable as a cause of action under Title VII of the Civil Rights Act of 1964. Then, only a few days later the EEOC issued an updated Enforcement Guidance that makes is more complicated, and more dangerous, for employers to utilize criminal background checks in their application and hiring process.

On April 23, the EEOC held that transgender workers are protected by Title VII. The decision came in the case of Mia Macey, a transgender woman who alleges that she was denied a job with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) after she disclosed that she was in the process of transitioning from male to female. The opinion is the first from the EEOC to specifically address whether or not transgender persons are protected. The EEOC is responsible for interpreting and enforcing Title VII on a nationwide basis. Employers in every state, including those that do not have statutory protections for transgender employees, can now face federal claims of discrimination by transgendered persons.

In reaching its decision, the EEOC reasoned that Title VII prohibits not just sex discrimination (that is, discrimination on the basis of biological sex), but any discrimination on the basis of gender stereotyping. In other words, the law prohibits employers from taking adverse employment actions against an individual because he or she fails to conform to any gender-based expectations or norms. Discrimination against a male who is presenting as a female, the Commission concluded, is just one type of discrimination that falls under sex discrimination.

By taking the position that Title VII protects transgender employees, the Commission has handed advocates for transgender rights a breakthrough victory. For more than a decade, advocates for the lesbian, gay, bisexual, and transgender community have been working to pass the Employment Non-Discrimination Act (ENDA), which would add sexual orientation to the categories protected by Title VII. The EEOC's ruling is likely to lend renewed momentum to the movement to pass the ENDA. This ruling is not binding upon court's, and it remains to be seen whether they will agree with the EEOC's position.

### What Can Employers Do to Protect Themselves?

Employers in jurisdictions where gender identity was not already protected prior to the Macey ruling should consider revising company policies and training programs to address this new risk.

# EEOC Issues Updated Enforcement Guidance on Consideration of Arrest and Conviction Records in Employment Decisions Under Title VII

On April 25, the EEOC issued updated Enforcement Guidance concerning employers' use of criminal arrest and conviction records when making hiring and other employment decisions. The EEOC Guidance states that, although Title VII does not bar the use of criminal background checks, employers may violate Title VII if (1) they intentionally discriminate, on the basis of race or national origin, against individuals with similar criminal histories or (2) their criminal background check policies have a disparate impact based on race or national origin, and they cannot demonstrate a "job-related business necessity" for those policies. While the Commission maintains that the updated guidance does not reflect a change in its policies, but merely updates and consolidates existing EEOC policies and guidance on the subject, the new guidance demonstrates the Commission's new commitment to investigating and pursuing enforcement actions in criminal background check cases. The guidance also demonstrates the risks associated with the application of broad, across-the board policies concerning the use of criminal background checks.

The updated Guidance explicitly states that criminal record exclusions have a disparate impact on minorities, especially African American's. The practical impact of the guidance is that employers, in defending their use of criminal history, may be limited to proving that their use of criminal background checks is "*job related and consistent with business necessity*." The updated guidelines state that the use of arrest and conviction records is "*job related and consistent with business necessity*" in two broad situations: (1) *when the employer validates its policy using the EEOC's Uniform Guidelines on Employee Selection Procedures*, and (2) *when the employer develops a targeted screen that considers the nature of the crime, the time elapsed since the commission of the crime, and the nature of the job for which an individual is applying and, the employer conducts an individualized analysis of the information gathered. This will usually entail informing individual applicants that they are being excluded on the basis of their criminal record, provide those applicants with an opportunity to explain their criminal records, and consider the explanations provided when deciding whether the use of the applicants' arrest and conviction records is, in fact, job related and consistent with business necessity.*

## What Can Employers Do to Protect Themselves?

Employers should conduct a thorough review of both their written policies concerning the use of criminal background checks in hiring and other employment decisions, as well as the practices used to implement those policies. As a part of that review, employers should consider the alternatives presented under the updated EEOC guidelines to demonstrate that their use of criminal background checks is consistent with Title VII. Those alternatives include taking steps to validate policies using the Uniform Guidelines on Employee Selection Procedures, and/or ensuring that the company's policies and procedures regarding the use of criminal histories provide for a targeted screen that considers (1) the nature of the crime, (2) the time elapsed since the commission of the crime, and (3) the nature of the particular job for which an individual is applying. ■

*Mr. Stovall concentrates his practice in the areas of labor & employment law, corporate formation, business, corporate and fiduciary litigation. Mr. Stovall represents individuals, private employers and public entities. Mr. Stovall is a frequent speaker, author and trainer, primarily in the areas of labor & employment law.*

# Executive Director's Message

*Erin H. Murphy*
*NADC Executive Director*

NADC membership numbers have remained steady over the past few years. As the 2nd quarter of the year comes to a close, let's take a look at the current membership statistics.

Membership currently stands at 484 members. Of those 484, 292 are full members, 160 are fellow members, 12 are trade association executive members and 20 are associate members. We have an outstanding crop of current members, but there is always room to grow.

NADC
National Association of Dealer Counsel

## *Welcomes New Members*

### Full Members

**John P. Hines**
The Hines Firm
*Atlanta, GA*

**Heather S. Thompson**
Dick Shirley Chevrolet, Inc.
*Burlington, NC*

### Trade Association / Executive Member

**Damon Lester**
National Association of Minority Automobile Dealers (NAMAD)
*Largo, MD*

The NADC relies on its members to act as ambassadors on behalf of the organization. NADC members are the organization's strongest supporters and most effective recruiters. The membership has a strong professional network that is invaluable.

Do you know an attorney, trade association executive or vendor who is not a member of NADC? The NADC works hard to assure that the membership has access to pertinent, up-to-date information and educational resources to help represent the best interests of your dealership clients. It is a win-win to get your colleagues involved!

As a refresher, please take some time to review the membership categories and the benefits associated with each:

**Full Member** – This membership category is for practicing attorneys who serve the needs of auto, truck, motorcycle, boat, motor home and all terrain vehicle dealers. Annual dues for Full Members are $585. Membership benefits include:

- Access to members-only meetings (registration fees required)
- Full access to website (including eForum and eLibrary) and list -serve
- Subscription to *Spot Delivery*®, a *CounselorLibrary* newsletter
- Subscription to *Defender*, the NADC newsletter

**Fellow Member** – This membership category is for members of organizations that already have one NADC Full Member or Trade Association Executive. Annual dues for Fellow Members are $200. Membership benefits include:

- Access to members-only meetings (registration fees required)
- Full access to website (including eForum and eLibrary) and list-serve
- Subscription to *Spot Delivery*®, a *CounselorLibrary* newsletter
- Subscription to *Defender*, the NADC newsletter

**Trade Association Executive Member** – This membership category is for those executives of the various trade associations (who are not lawyers) that represent the industry. Annual dues for Trade Association Executive Members are $585. Membership benefits include:

- Access to members-only meetings (registration fees required)
- Full access to website (including eForum and eLibrary)and list-serve
- Subscription to *Spot Delivery*®, a *CounselorLibrary* newsletter
- Subscription to *Defender*, the NADC newsletter

**Associate Member** – This membership category is reserved for companies and organizations that support the NADC and are interested in furthering NADC goals. Annual dues for Associate Members are $1,500. Membership benefits include:

- Access to members-only meetings (registration fees required)
- Promotional opportunities at NADC events
- Advertising opportunities in NADC publications
- Subscription to *Spot Delivery*®, a *CounselorLibrary* newsletter
- Subscription to *Defender*, the NADC newsletter

If you know a colleague or industry partner that would benefit from NADC membership, please contact Erin Murphy at emurphy@dealercounsel.com. We will happily send out a prospective member informational packet to all interested parties. Please note that membership dues are good for a year from the month the member joins, they do not expire at the end of the calendar year.

Help us reach our goal of 500 members by the close of 2012!! ■

# Recent FTC Action Confirms Importance of Safeguards Diligence

Feature Article

*By Michael Charapp, Charapp & Weiss, LLP*

On June 7, 2012, the FTC announced that it had agreed on terms of a consent order with a Georgia Toyota dealer stemming from the dealer's failure to maintain adequate control of its customer information as required by the FTC Safeguards Rule. http://www.ftc.gov/os/caselist/1023094/120607franklinautomallagree.pdf. The FTC charged that the dealer had violated its Safeguard obligations by loading peer-to-peer (P2P) software onto its computer system. The effect of this, the FTC charged, was to open up much of the dealer's computer data, including non-public personal information of consumers with whom the dealer had done business, to others on the file sharing network. The FTC charged that this violated the Safeguards Rule's requirement to have in place protections against open availability of private customer information and was contrary to the privacy notice issued by the dealer which assured that it had such protections in place.

The consent order requires the dealer to follow specific compliance procedures for twenty years. Not only must the dealer put the procedures in place, train its employees about them, and regularly monitor compliance, it must retain an outside certified expert to do an initial assessment and a follow up assessment every two years to be sure that the dealer's process is being followed. Like all FTC consent orders, it is backed up by the FTC's power to level civil penalties for violations.

The FTC consent order shows one reason why dealers must protect non-public customer information – the law requires it. However, there is an even more compelling reason for dealers to do so – customer data is a valuable asset.

Whenever a factory repurchases a dealer's franchise, it always wants a computer readable copy of the dealer's customer information. Dealers often ask why, since the factory already has information on every customer who bought a new car. There apparently are reasons for this (the factory does not have used car buyer information, the information it has may not have the breadth of information carried on the dealer's system, and others). But whatever reason, the factory sees this information as so valuable that it will generally not do a deal to buy back a dealer's franchise for which it pays hundreds of thousands or even millions of dollars without receiving this information. So what does that tell us about dealers' customer information? Simply that it is part of the six or seven figure goodwill value of any franchised dealership. A dealer would not leave hard assets, like cars or cash, of this value lying around unprotected in an unlocked space for anyone who wants to come in and make off with them. It protects these valuables very carefully. So why is it any different with customer information?

Given the stakes, it is important that dealers give careful attention to the protections they have in place for their customer data. As the Georgia dealer found the hard way, adding P2P software to the dealer's computer system is a major problem. It improperly opens to anyone on the file sharing network internal data of the dealership, including customer data that must be protected. But there are other areas of vulnerability to which dealers may not be giving enough attention. Here are two of them.

## Vendor Agreements

There are a lot of marketers out there claiming that they perform magic. There is no end to those who claim to have a secret formula to get customers to flock to a dealer's showroom. Whether it is a

program to attract customers who haven't been in for a while, or a plan to bring in customers based on a pitch to refinance their loans, or a system to prospect existing customers to sell them a second car, they all have one thing in common. If dealers will simply provide them with access to their customer information, they can sit back and watch the magic happen! Unfortunately, the only magic a dealer may see is the equity in its customer list disappearing.

It is puzzling how willing dealers are to give vendors with whom they have no experience access to customer information. Sure, a marketer may provide an agreement under the FTC Safeguards Rule that it won't misuse the non-public private information of your customers. But what good is that from a company that may have little or no assets? What good is that from a company that may fold at any time and be reconstituted with a new name at a new address?

Customer information is a valuable asset of any dealership. Simply the data on buying patterns and pricing can be sold to companies who market the results. The actual names, addresses, email addresses, and phone numbers of customers are much more valuable. Why risk making that available to someone a dealer knows little about?

Any dealer wishing to do business with a marketer who will have access to customer information should be careful. The first step, without question, is to get a safeguards agreement pursuant to the FTC Rule. The Rule requires that. But a dealer should do much more.

Check out the vendor. Where is it located? What does a rating service have to say about it? Are its references real, are they actual car dealers, and what do they have to say about the company? Does the company have bank references? Does the company have vendor references?

Limit access to the DMS. Once in the DMS, the marketer can take any information it wants.

Even when pushing information from the DMS, the information should be selected carefully. For example, in a promotion to customers whose financing is maturing just push that customer data. A dealer should not give out its whole customer list and allow the vendor to sort it.

The agreement a dealer signs with the supplier should carefully define the use to which the supplier can put the information. What limits on the use of the information are included? If there is misuse and the dealer needs to sue, can it file suit in its own home town or must it go across the country to sue?

Is the vendor willing to include in its agreement that it will not use any of the information for any purpose whatsoever other than to provide services to the dealer? Often, companies will agree to protect private customer information but it will develop information profiles from data that it will market. If a dealer does not want this, it must get an agreement that the supplier will not do this.

## *SAVE THE DATE for the*

## *2012 NADC Fall Conference October 7-8, 2012*

*Trump International Hotel & Towers*
*Chicago, IL*

### Hotel Reservations

Reservations must be made directly with the Trump International Hotel & Tower by calling 1-877-45-TRUMP. Please reference the 2012 NADC Fall Conference to receive our discounted rate of $265 a night. A deposit equal to one night's stay is required to hold each individual's reservation.

**The room block deadline for hotel reservations is September 17, 2012.**
*Space is limited so make your reservation today!*

If you have any issues reserving your room please contact Erin Murphy at: emurphy@dealercounsel.com for assistance.

### Topic Suggestions

*Are there specific topics you would like to see covered at the NADC Fall Conference?*
If so, please email Erin Murphy with your suggestions.

## Physical Security for Computer Access

Under the FTC Safeguards Rule, a dealer must have physical security for customer information kept in tangible media such as documents and files. That is why dealers, when the Safeguards Rule became effective, spent substantial time and money making sure that file cabinets were locked, the general office was secured, and locks were installed on F&I office doors, among dozens of other protections.

Similarly, under the Safeguards Rule a dealer is required to provide computer security for data kept and transmitted electronically. A dealer's computer vendor can help provide online security for this data. The DMS system should not provide open access to customer data to every authorized system user. That is not just a requirement of the FTC Safeguards Rule, it is also good business sense and good common sense. Just because employees have the authority to look up service tickets, or selected deal information, they should not have the opportunity to access or to start downloading all other information. The computer vendor can help with that.

However, there is one vulnerability that may be overlooked for electronic data – physical security. A recent lawsuit filed in Pennsylvania between two law firms is instructive in this area. Earlier this year, a partner in a law firm decided to leave his firm and take his practice to another firm. Knowing that the firm he was exiting could object and might seek to block him if he took files, he allegedly went in after business hours with a tech savvy friend. The friend hooked up a portable hard drive to the firm server and downloaded hundreds of thousands of client documents. The firm he left was not amused when it found he took these files to his new employer. It sued the attorney, two other firm employees who left with him, his techie friend, and the hiring law firm. As this is written, the battle is going on.

So what should one take from this? Some dealers have not migrated to cloud-based DMS systems; they still have servers on the premises. The server may be in an equipment room that is left open so that employees may access the server or other equipment in the room. If many people can access it, so can an employee with a portable hard drive intent on no good. All server equipment must be locked up and secured.

In addition, in cloud-based systems, full access may be available from any computer on the system by someone using the proper credentials. Dealer managers, such as the General Manager or the Controller, who have full access to the system should have their computers in offices that are locked and secured. Passwords or other log on keys should never be left in plain sight (a sticky note on a monitor screen) or where a thief would expect to find it (in desk drawers or under a desk blotter near the computer).

Computer security has come a long way, but basic physical security measures for computer equipment and access may be overlooked.

## The Importance of Regular Audits

A dealer's Safeguards system is only as good as its ability to respond to the latest threat. Whether it is P2P software, hacker threats, or simply lack of physical security for access to computer data, new threats can arise regularly. That is why the FTC Safeguards Rule requires that a business conduct regular audits to determine the effectiveness of its policy and procedures. From time to time, a dealer must look at its system to determine whether there are threats against which it has not protected itself, what incidents may have occurred that require changes, what experiences dealership personnel have had that suggest amendment to the plan or procedures are necessary, or for other potential information leaks. Hopefully, all dealers have adopted a Safeguards compliance plan. But a dealer who does not regularly review and revise the plan and procedures is not effectively protecting its customer data and its business. ■

*Michael G. Charapp is a lawyer in the Washington, D.C. metro area who represents car dealers and dealer associations. He is editor of the Defender and encourages submissions.*
*Email:* mike.charapp@cwattorneys.com.

# DEFENDER – Advertising Opportunities

*Defender, The NADC Newsletter is published by the National Association of Dealer Counsel*

**Yes!** I would like to purchase an ad in the *NADC Defender.*

☐ ½ page ad $150.00
5″ high x 7.5″ wide, no bleeds

☐ ¼ page ad $100.00
5″ high 3.75″ wide, no bleeds

**Issue Months:**

☐ July/August 2012 ☐ September 2012
☐ October 2012 ☐ November 2012
☐ December 2012

Contact: _____

Company: _____

Address _____

Phone: _____

Email: _____

**Method of Payment**

☐ Check ☐ Invoice me
☐ American Express ☐ Mastercard ☐ Visa

_____
Credit Card No.

_____
Expiration Date

_____
Signature

**Send to:**
NADC, 1155 15th Street, NW, Suite 500, Washington, DC 20005, Phone: 202-293-1454, **Fax: 202-530-0659,** www.dealercounsel.com
**Questions:** Erin Murphy, email: emurphy@dealercounsel.com

## *BE A CONTRIBUTOR!*

***We are always looking for submissions to publish in the Defender. Please send your contributions or proposals for articles to:***

***mike.charapp@cwattorneys.com***

NADC
NATIONAL ASSOCIATION OF DEALER COUNSEL

**Volume VIII, Number 6**
**JUNE, 2012**

**Michael Charapp, Editor**
mike.charapp@cwattorneys.com

**Trudy Boulia, Assistant Editor**
tboulia@jpharveylaw.com

*Defender, The NADC Newsletter is published by the National Association of Dealer Counsel*
1155 15th Street, NW, Suite 500, Washington, DC 20005
Phone: 202-293-1454 • Fax: 202-530-0659 • www.dealercounsel.com