THE WANADA BULLETIN
NEWS AND INFORMATION FOR AND ABOUT FRANCHISED NEW CAR DEALERS IN THE WASHINGTON AREA
WANADA Bulletin # 20-22 **November 16, 2022**

WANADA Annual Meeting: New Format Energizes Premier Event

Reformatted as a dinner for the first time in recent memory, the 2022 WANADA Annual Meeting was, by any measure, a smashing success.

"We wanted to change it up and present the Annual Meeting in the style of WANADA's Centennial Dinner a few years back," said WANADA CEO John O'Donnell. "Our intention was to have a dinner with special entertainment every few years, but after the feedback we've received, we might just do this every year!"

WANADA Chairman Chip Doetsch (center), flanked by his father, former chairman George Doetsch (left) and former WANADA CEO Gerry Murphy (right)

The event, which was held at Columbia Country Club in Chevy Chase, MD, began with cocktails at 5:30 p.m. The room quickly filled with over 200 dealership principals and senior managers saying their hellos and examining the $6,500+ diamond earrings that were being raffled to benefit the Automobile Dealer Education Institute (ADEI). Right at 6:30, the chimes rang and the doors were opened for the main dining room.

After a brief welcome from John O'Donnell, dinner was served, during which the guests were treated to an informative and entertaining presentation from keynote speaker Glenn Mercer. Mercer, a well-known automotive industry analyst, regaled the audience with insightful facts on the future of automotive retailing, punctuated with his remarkably dry wit. Mercer encouraged the gathered dealers to not buy into the hype of Wall Street or so-called industry "disrupters" that see the future of car selling as factory direct, and instead provided data that strongly indicates the

franchise system as the best sales and service model for American consumers. Mr. Mercer also pointed out that the biggest growth area in a dealership is the service department and provided some broad insights into how market share might be reclaimed from the aftermarket.

Clockwise from top left: Jim Willard, Mike McNicholas and Farokh Bagha from EuroMotorCars; WANADA CEO John O'Donnell, keynote speaker Glenn Mercer and comedian Tom Shillue

Following the keynote address, WANADA Chairman Chip Doetsch of Apple Ford in Columbia, MD, delivered a "state of the association" address. Mr. Doetsch referenced the recent challenges surrounding the COVID pandemic and global supply chain as a "laboratory" in which the franchise system was proven remarkably durable. As such, he continued, the impending challenges dealers face from overreach at the federal level, while daunting, would ultimately prove dealers' resourcefulness and ability to overcome even remarkable hurdles. Chairman Doetsch applauded WANADA's leadership for their continued advocacy at the state, local and federal level, and called upon the dealers to increase their support of the association's activities. Such a robust slate of member services and political action, he explained, comes at a cost. By supporting the association's insurance business and advocating on behalf of the Washington, DC Auto Show with their respective OEMs, each dealer can play a part in keeping the industry strong. Chairman Doetsch then closed his remarks by noting that the dealers in attendance were clearly among the engaged and asked that each attendee reach out to a fellow dealer who was not fully engaged with WANADA and seek to bring them along.

Following the Chairman's Address, Immediate Past Chairman Kevin Reilly of Alexandria Hyundai and Genesis took the podium to commence the business portion of the evening. Reporting from his role as Chairman of the Nominating Committee, Mr. Reilly noted that Robert Farrell of Penske Automotive and Jim Gramm of Safford Auto Group had each completed two terms as Directors and would be rolling off the Board. After thanking Messrs. Farrell and

Gramm for their service, Chairman Reilly continued that the Committee had nominated Bill Colgate of Jaguar-Land Rover of Annapolis and Melody Lesane of RRR Automotive as Directors in their place. The new Directors were then officially added by vote of acclamation.

Once the business of the evening had been attended to, guests were treated by a highly-entertaining set of stand-up comedy from Daily Show alum and Gutfeld regular Tom Shillue. Shillue had the crowd in stitches as he recalled seemingly offensive 70s jingles and his humorous take on the challenges of raising daughters in the midst of "woke" culture. To close the evening, Tom Parsons of B&R Associates raffled off the aforementioned pair of diamond earrings to one lucky attendee, who was thrilled to be the winner considering his wife's birthday was just around the corner!

WANADA would like to especially thank the support of the generous sponsors who helped make the 2022 Annual Meeting such a smash hit: BG Crovato Products & Services, Chesapeake Contracting Group, Citrin Cooperman, Penney Design Group, The Keats Group at RBC Wealth Management, and Truist.

WANADA Dealers Invited to Join Fraud Prevention Webinar

The Northeast Regional Chapter of the International Association of Auto Theft Investigators (IAATI) has invited WANADA dealer members to join its upcoming webinar on fraud prevention: November 17 @ 2:00 p.m. Registration is available here.

This webinar will cover an analysis of fraud patterns and trends uncovered in the auto lending fraud consortium - a vast database containing over 130 million auto finance applications from across the country. The analysis reveals that the industry can expect over $8 billion in auto fraud risk this year, including schemes to defraud lenders and dealers through income fabrication, use of fake employers, synthetic identities, straw borrowers, ghost loans, powerbooking, and insider fraud.

The presenter will be Frank McKenna of Point Predictive. Frank McKenna is the Chief Fraud Strategist of Point Predictive and the author of FrankonFraud, a blog covering global fraud trends. He has worked with over 250 banks and lenders in the US, helping them integrate AI solutions to combat fraud and risk.

FTC Extends Compliance Deadline for New Safeguards Rule

The Federal Trade Commission today announced it is extending by six months the deadline for companies to comply with some of the amendments to the FTC's Safeguards Rule. Earlier this year, NADA submitted comments to the FTC seeking an extension of the deadline. The deadline for complying with some of the updated requirements of the Safeguards Rule is now June 9, 2023.

The provisions of the updated rule specifically affected by the six-month extension include requirements that covered financial institutions:

- designate a qualified individual to oversee their information security program,
- develop a written risk assessment,
- limit and monitor who can access sensitive customer information,
- encrypt all sensitive information,
- train security personnel,
- develop an incident response plan,
- periodically assess the security practices of service providers, and
- implement multi-factor authentication or another method with equivalent protection for any individual accessing customer information.

Dealers are encouraged to continue in their efforts to expeditiously comply will all the new requirements of the Rule but should consult with their attorneys, service providers and IT professionals about the potential impact of this deadline extension.

For more information on the FTC Safeguards Rule, click here.

From NADA: New EEOC "Know Your Rights" Posters

The Equal Employment Opportunity Commission (EEOC) recently released a new "Know Your Rights: Workplace Discrimination is Illegal" poster to replace one entitled "EEO is the Law." Dealerships must prominently display the latest version of the "Know Your Rights" poster in conspicuous locations at their worksites. Such locations include poster boards accessible to applicants and employees with disabilities and employee websites.

The EEOC administers and enforces federal laws designed to protect workers against employment discrimination. The "Know Your Rights" poster is written to provide information on federal anti-discrimination law to applicants, employees, and employers. It stresses that federal law prohibits job discrimination based on race, color, sex (including pregnancy and related conditions, sexual orientation, or gender identity), national origin, religion, age (40 and older), equal pay, disability, or genetic information (including family medical history or genetic tests or services). It also notes that employers may not retaliate against an employee for filing a discrimination charge, reasonably opposing discrimination, or participating in a discrimination lawsuit, investigation, or proceeding.

General questions regarding the EEOC poster may be directed to regulatoryaffairs@nada.org.

The FTC's rapidly evolving standards for MFA

In light of the FTC's recent policy pronouncements and apparent unwillingness to engage in helpful dialogue with industry interests, it is prudent for dealers to stay vigilant on issues that may affect them down the road. Another issue that appears to be gaining some traction within the FTC centers around cybersecurity. The article below, originally published on iapp.org, discusses "multi-factor authentication" and possible ramifications of the FTC's approach to business' responsibilities in safeguarding customer data.

###

Two recently settled enforcement actions by the U.S. Federal Trade Commission, combined with new guidance from the Cybersecurity and Infrastructure Security Agency, represent a big leap forward in the expectations placed on data custodians for use of multifactor authentication. Read together, they require privacy and information security professionals to reassess their organizations' approaches to controlling employee, contractor and affiliate access to enterprise systems that contain personal information.

Remind me again: What is MFA?

First, a refresher. Authentication is the process of proving identity. In the digital context, it is often a prelude to accessing a system. As CISA succinctly explained in its Oct. 31 guidance, MFA is a security control that requires system users to present a combination of two or more different types of authenticators (something you know, something you have or something you are) to verify their identity for login.

For years, it has been recognized that passwords (where the password is one form of authentication, i.e., something you know) are woefully vulnerable. The methods available to hackers to compromise password-based access controls continue to grow. Combining passwords with security questions doesn't help much, since you are still relying on only one type of factor (something you know).

A second factor, such as a physical item you possess (a cell phone, smart card or hardware key) or a biometric (something you are) can provide better security. That's multifactor.

More enterprises are using MFA in at least some contexts, and many online services offer MFA to their customers as an option. Many of these systems, especially the consumer-facing ones, rely on numeric codes sent by text to one's cell phone or on push notifications to mobile applications.

Bad news: Many approaches to MFA are vulnerable

However, there is growing recognition that many approaches to MFA (including short message service text and push notifications) are themselves vulnerable. As the White House's Office of Management and Budget warned in a January memorandum to government agencies, "sophisticated phishing attacks … can convincingly spoof official applications and involve dynamic interaction with users. Users can be fooled into providing a one-time code or responding to a security prompt that grants the attacker account access. These attacks can be fully automated and operate cheaply at significant scale."

The FTC's evolving approach

In its Oct. 24 settlement with online alcohol marketplace Drizly and its CEO over allegations that the company's security failures led to a data breach exposing the personal information of 2.5 million consumers, the FTC drew on this awareness. The regulator ordered the company to require MFA for all employees, contractors and affiliates in order to access any assets — including databases — storing customer information. Moreover, the commission specified that the MFA methods must be resistant to phishing attacks.

Likewise, in a settlement announced just a week later with educational technology provider Chegg for its lax data security practices that exposed sensitive information about millions of its

customers and employees, the commission again ordered the company to require phishing-resistant MFA for all employees, contractors and affiliates accessing customer information.

What is phishing-resistant MFA?

The FTC's emphasis on phishing-resistant MFA takes on added significance — and compliance becomes much more complicated — in light of the CISA guidance, released on the same day as the FTC's Chegg announcement. CISA repeated warnings that some forms of MFA "are vulnerable to phishing, 'push bombing' attacks, exploitation of Signaling System 7 (SS7) protocol vulnerabilities, and/or SIM swap attacks." Specifically, CISA discouraged the use of SMS or voice MFA, which works by sending a code to the user's phone or email.

"This form of MFA," the agency said, "should only be used as a last resort MFA option. However, it can serve as a temporary solution while organizations transition to a stronger MFA implementation." But CISA also made it clear that app-based authentication is vulnerable, depending on specific type, to phishing attacks or push bombing.

CISA stated that there is only one widely available form of phishing-resistant authentication: the Fast ID Online/Web Authentication standard developed by the FIDO Alliance and published by the World Wide Web Consortium. I'm just a lawyer, so I've reached here the limits of my technical understanding. Determining which products use FIDO/WebAuthn and how it can be effectively implemented will require some careful scrutiny by privacy and information security professionals in conjunction with their IT colleagues. Further guidance from CISA and/or the FTC would be very helpful, especially given the legal risk to data custodians if it turns out their MFA is not, in fact, phishing-resistant.

CISA also noted that there is another form of phishing-resistant MFA tied to an enterprise's Public Key Infrastructure, but it requires highly mature identity management and is sensible mainly for large and complex organizations. As CISA noted, a well-known form of PKI-based MFA is the smart cards called PIV cards that federal government agencies use to authenticate users to their computers.

Remember, of course, phishing-resistant MFA is not "un-phishable." As with almost all other cybersecurity controls, we're talking risk mitigation, not risk elimination.

Evolution

Overall, the two FTC cases combined with the CISA guidance represent a major evolution in the commission's view of authentication. MFA first made an appearance in FTC enforcement actions in 2019 when the commission required Equifax to implement access controls across its network, "such as multi-factor authentication and strong password requirements."

Just about a year ago, in its revised Safeguards Rule under the Gramm-Leach-Bliley Act, the FTC required the financial services entities it regulates to implement MFA but declined to specify what forms of MFA were adequate. The commission specifically declined to rule out SMS text messages as a viable solution. And just four months ago, when the FTC required CafePress to adopt MFA, it specifically cited mobile authenticator apps as an appropriate method. Now, the FTC has specifically prohibited Drizly from using telephone or SMS-based MFA and the CISA guidance flatly says that to be phishing-resistant, an MFA method must either use WebAuthn or be linked into an organization's PKI.

This comes after a rising tide of concern about phishable MFA. Recent high-profile examples include a campaign targeting Github users, which someone at Dropbox succumbed to. Accordingly, in the January memorandum to agencies on the topic, the OMB told agencies that, for routine self-service access by agency staff, contractors and partners, they must "discontinue support for authentication methods that fail to resist phishing, including protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications."

Key distinction: enterprise users in contrast to customers
Until the recent pair of decisions involving Drizly and Chegg, the FTC was pretty unclear in its orders regarding MFA by failing to distinguish between access by consumers or customers and access by enterprise users (employees, contractors and affiliates). In the latest orders, the commission drew a clear distinction.

Drizly and Chegg are required to adopt phishing-resistant authentication for all employees, contractors and affiliates in order to access assets (including databases) containing customer information, but the companies are only required to offer MFA as an option for consumers without a requirement that it be phishing-resistant. Likewise, the OMB requires phishing-resistant MFA for agency staff, contractors and partners, but phishing-resistant MFA need only be an option for public users.

The CISA guidance makes it clear why this distinction is so important. Implementing phishing-resistant MFA is not easy. Achieving it for employees, contractors and affiliates accessing databases with personal information will be hard enough. Requiring it for millions or hundreds of millions of individual consumers would be impossible. Small and medium-sized entities will likely struggle to keep pace for employee access.

Like all of cybersecurity, the recent FTC and OMB decisions to mandate phishing-resistant MFA for employees are risk-based. If an individual customer gets phished, only their own money or data are at risk. Nothing to be blasé about, but the scope of the threat is confined. If an employee at an enterprise or agency who has access to a database containing the data of millions or more individuals gets phished, the risk is catastrophic.

How broadly should MFA be applied?
The FTC takes a very broad view of what personal information requires protection. We're way beyond the days of narrowly defined personally identifiable information or sensitive PII. The Drizly case is only the most recent one driving this home. There, the compromised databases contained names, email addresses, postal addresses, phone numbers, unique device identifiers, order histories, partial payment information, geolocation information and consumer data (including income level, marital status, gender, ethnicity, children and home value) purchased from third parties. It contained no Social Security numbers or full credit card numbers, which are the traditional building blocks of identity theft.

Nevertheless, the FTC concluded that malicious actors combine the kinds of information taken from Drizly to perpetrate fraud or obtain additional personal information by impersonating companies with whom the target has previously transacted. This, the commission concluded, provided sufficient cause for it to allege an illegal unfair and deceptive trade practice by Drizly. So one has to assume that the new preference for phishing-resistant MFA applies to all systems and databases with personal information, broadly defined.

Policy implications

Opponents of the government regulating cybersecurity have long argued that the technology of attack and defense is changing so rapidly that government agencies could not possibly keep up. The rapid evolution of the FTC's approach to MFA provides evidence for precisely the opposite policy conclusion: Profit-driven companies, notoriously under-investing in security, need government prodding to respond to rapid changes in the technology of attack and defense, and agencies like the FTC are showing themselves perfectly able to increase their expectations on data custodians.

Might there come a time, perhaps very soon, when all existing forms of MFA are vulnerable? Even in 2003, a National Academies study advised that MFA techniques were not foolproof. Indeed, Dropbox reported Nov. 1 that it had been the victim of a successful phishing attack that got around a hardware authentication key. Accounts protected by hardware security keys are supposed to be invulnerable to "man-in-the-middle" attacks, but the incident along with the overall trend in cybersecurity suggests that yes, attackers may render the universe of phishing-resistant MFA a null set. But that is just another reason for the type of regulatory adaptation we see in the recent FTC cases.

MFA could be the poster child for the FTC's case-by-case approach to cybersecurity. As Dan Solove and Woody Hartzog convincingly argued almost a decade ago, the FTC's privacy and cybersecurity complaints and settlements constitute a body of common law, evolving just as judicially decided law does. As such, they define at any given moment the legal obligations on data custodians. Thus it is with the FTC's approach to MFA, although the pace of evolution is — in line with other aspects of the digital age — far more rapid than it ever was with traditional common law. As the FTC approaches its nascent rulemaking on privacy and data security, it should keep in mind the flexibility that case-by-case enforcement allows the FTC to rapidly signal changes in its expectations for data custodians.

The WANADA Bulletin is Sponsored by the Following Kindred-Line Members: