The FTC's Proposed Data Breach Settlement with a DMS Provider: What It Means for Dealers

Proposed FTC-DealerBuilt Data Breach Settlement

The Federal Trade Commission (FTC) recently announced that it has entered into a proposed consent order with a dealer DMS provider (LightYear Dealer Technologies, dba "DealerBuilt") to settle allegations that it "failed to implement readily available and low-cost measures to protect personal information it obtained from its auto dealer clients." According to the FTC, this "led to a breach that exposed the personal information of millions of customers." The FTC maintains that this failure constitutes (i) an unfair practice under the Federal Trade Commission Act, and (ii) a violation of the Gramm Leach Bliley Act (GLB) Safeguards Rule, because the DMS provider is a "financial institution" under the rule and is required – similar to its auto dealer clients – to fulfill a series of information security requirements set forth in the rule. The proposed consent order – which is explained here and must be approved by the FTC following a public comment period – imposes a series of data security requirements on the DMS provider.

What Should DealerBuilt Dealers Focus On?

The FTC's complaint against DealerBuilt stated that "[d]ealership customers and consumers had no way of independently knowing about [DealerBuilt's] security failures and could not reasonably have avoided possible harms from such failures." Nonetheless, it is very important that dealer customers of DealerBuilt work with their attorneys to ensure that they take all appropriate steps under state and local law and their contracts in response to this announcement.

What Should All Dealers Focus On?

No auto dealer was named in the FTC's action against DealerBuilt. However, the action highlights a broader concern for all dealers, which is the need to be proactive in ensuring that all dealer service providers (meaning any person or entity that receives, maintains, processes, or otherwise is permitted access to the dealer's customer information while providing services to the dealer) are taking appropriate steps to secure the dealer's customer data. This includes employing measures to protect such data both **in transit** and **at rest** (which generally refers to data when it is stored on a computer system).

Since 2003, the Safeguards Rule has required dealers and other financial institutions to develop, implement, and maintain a comprehensive written program to protect their customer information. The program must have five elements, one of which is the need to –

1) take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the financial institution's customer information, and
2) require these service providers by contract to implement and maintain such safeguards.

Addressing Service Provider Requirements

With regard to how the ***first part of the service provider requirement*** applies to DMS providers, the FTC's complaint against DealerBuilt is instructive and identifies areas that dealers, in consultation with their counsel,

should review with their DMS providers and other service providers. In particular, the FTC's complaint alleges that the DMS provider failed to provide reasonable security for the customer information stored on its network in part by –

a) failing to develop, implement, and maintain a **written information security policy**;
b) failing to implement reasonable guidance or **training** for employees or third-party contractors, regarding data security and safeguarding customer information;
c) failing to **assess the risks** to the personal information stored on its network, such as by conducting periodic risk assessments or performing vulnerability and penetration testing of the network;
d) failing to use readily available measures to **monitor** its systems and assets at discrete intervals to identify data security events (such as unauthorized attempts to exfiltrate consumers' personal information across the company's network) and verify the effectiveness of protective measures;
e) failing to impose reasonable **data access controls**, such as restricting inbound connections to known IP addresses and requiring authentication to access backup databases;
f) storing consumers' personal information on its computer network **in clear text**; and
g) failing to have a reasonable process to **select, install, secure, and inventory devices** with access to personal information.

Dealers should consider using the foregoing as a **checklist** of the types of protections that service providers need to employ relative to the data they handle for their dealer customers.

With regard to the ***second part of the service provider requirement***, NADA issued several years ago a sample service provider contract addendum that a dealer could use or incorporate into its service provider contracts. (The addendum, along with important limitations and disclaimers, is available at www.nada.org/dealerdata.) It generally states that the service provider will (i) only access/store/transmit/etc. the data required to provide the service for which it has been retained, (ii) only use the data to provide this service, and (iii) take appropriate steps to safeguard the data. However, recent developments highlight the importance of addressing other important matters in contracts with service providers, including (i) specific technical issues such as encryption, vulnerability assessments, penetration testing, incident response plans, and disaster recovery plans, and (ii) other important issues such as the dealer's ability to conduct regular audits of the service provider's safeguarding procedures, data breach obligations and requirements, indemnification, cyber-liability and other insurance requirements, and any specific duties imposed by state law.

Conclusion

In short, while the FTC's proposed consent order with DealerBuilt makes clear that dealer DMS providers have a **direct** responsibility for data security, it also underscores – and provides detailed guidance regarding – the dealer's data security obligations under the Safeguards Rule and, in particular, the requirement that it oversee the dealer's service providers. Satisfying the service provider requirement requires more than signing an agreement with a vendor stating that it complies with the Safeguards Rule. **Dealers must – both at the time of vendor selection and periodically thereafter – have a reasonable process in place to ensure that each of its vendors with access to its customer information is capable of protecting that information.**

The foregoing is provided for informational purposes only and is not intended as legal advice. Dealers should consult counsel familiar with their operations and applicable federal, state, and local law for advice on appropriate information security compliance measures to adopt for their dealership.