

EXHIBIT “C”

finance&insurance

Get the F&I Report delivered via email each Wednesday. Sign up at autonews.com/fireport.

Former exec: CareGard bungled data breach

F&I company says it had no obligation to report beyond FBI

John Huetter
john.huetter@crain.com

A finance and insurance provider was unprepared for a ransomware attack last summer and for months failed to alert automaker partners and agents selling its coverage to dealerships, a whistleblower alleges.

Travis Gates was president of AFG Technologies, which developed software for CareGard Warranty Services Inc., for more than a decade before resigning April 5. He said he worked to rebuild CareGard's systems after an attack was discovered in August. A hacker or hackers allegedly encrypted 105,910 files from CareGard, a finance and insurance products provider that Gates estimated had ties to at least 1,000 dealerships, and threatened to publish information they claimed they downloaded.

Gates provided Automotive News with multiple internal emails from AFG Cos., the parent of AFG Technologies and CareGard, which described the breach and the company's response. Gates said that after his resignation, he alerted attorneys general in 48 states and CareGard customers in-

cluding Nissan, Southeast Toyota Distributors and Mercedes-Benz about the breach.

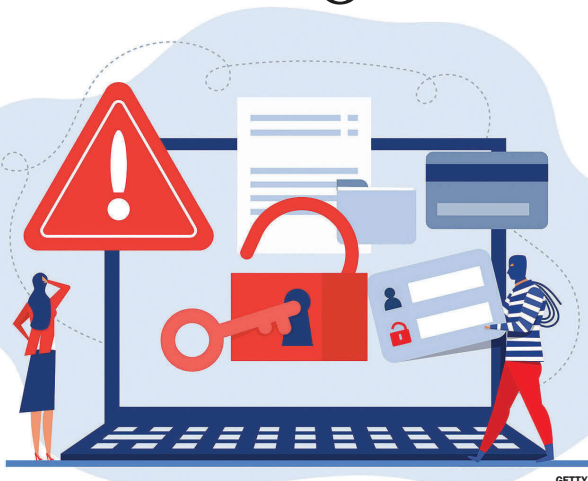
"I don't want to be in this position," Gates told Automotive News. "I definitely don't have any offense against anybody there."

In a statement shared with Automotive News last week, CareGard said it was told Aug. 13 by cybersecurity information technology firm Integrus that "our anti-virus caught a ransomware attack" and acknowledged files had been encrypted. But it said its IT team and cybersecurity firm Booz Allen Hamilton "extensively reviewed the encrypted files and did not identify any access to personal information protected under state law for employees, customers, or any other groups of individuals."

CareGard said Booz Allen Hamilton continues to monitor the Internet for leaks but found no "mention of AFG Companies or any of its subsidiaries to date."

Extent may be unknown

Gates alleges a CareGard employee accidentally wiped out internal access logs for the files after the incident and that AFG Cos. rejected Booz Allen Hamilton's recommendation to contact the attacker. Thus, it has no idea if any other records were compromised besides the encrypted files, according to Gates. He said contractual relationships and the Federal Trade Commission's Safeguards Rule would dictate alerting business partners.



and "fully engaged" Integrus for cybersecurity following the breach. Gates agreed CareGard's cybersecurity is now robust.

A breach and threat

Gates said CareGard was alerted of the breach Aug. 13 — two months after auto dealerships and other federally classified "financial institutions" were to be in compliance with new detailed Safeguards Rule requirements originally approved by the FTC in 2021. Gates argues CareGard should have held itself to the same standard so as not to leave its partners' data exposed.

The update also added a requirement that financial institutions periodically check the security and risk of service providers such as CareGard.

On Aug. 15, a sender known as "alphv.alphv" emailed Wright Brewer, CEO of AFG Cos. and CareGard, and announced it had breached the CareGard system and threatened to release data, according to an email Gates provided to Automotive News.

Gates alleged the attacker was affiliated with Blackcat, which the Justice Department in December said over the prior year and a half had become "the second most prolific ransomware-as-a-service variant in the world based on the hundreds of millions of dollars in ransoms paid by victims around the world." Blackcat also

Neither current nor former versions of the Safeguards Rule discuss disclosing a breach to potentially affected parties. However, the FTC website advises businesses that suffer a breach to have a plan for sharing information with "all affected audiences — employees, customers, investors, business partners, and other stakeholders. Don't make misleading statements about the breach. And don't withhold key details that might help consumers protect themselves and their information. Also, don't publicly share information that might put consumers at further risk."

According to Gates, at the time of his resignation, CareGard had not contacted the FBI, state regulators, its cli-

ents or the F&I agents selling products to dealerships. Potentially affected companies would include Southeast Toyota, Nissan and Mercedes-Benz, he said.

CareGard said it reported the attack to the FBI following the recommendation of law firm Mullen Coughlin. In a follow-up statement, it said the report was made Aug. 17. The FBI declined to comment on the timing.

"AFG/CareGard was advised it had no further reporting obligations," the company said in its original statement. The company had not responded to a request for clarification on whether business partners ultimately were informed, and if so, when.

CareGard said it replaced hardware

see CAREGARD, Page 16

Ill. court blocks floorplan collection

The dealers allege the bank took part in fraud scheme

Eric Freedman
autonews@crain.com

A floorplan lender remains blocked from collecting about \$2.8 million from an Illinois dealership and its owners in a dispute involving allegations the bank participated in a fraud scheme by store employees behind the dealers' backs.

The Appellate Court of Illinois refused to lift a preliminary injunction preventing the Bank of Herrin from foreclosing on collateral from Ward Chrysler Center in Carbondale and principals Ronald and Mark Ward.

The bank was the floorplan lender for the Wards' Chrysler store and their Chevrolet store in Metropolis, Ill., from 2016 to 2018, according to the unanimous decision written by Justice Thomas Welch. In 2017, employees at the Chrysler store started dou-

ble-booked loans — requesting multiple loans from the Bank of Herrin for the same vehicles, the decision said.

"These double-booked loans were part of a scheme in which the employees sold new vehicles at a reduced rate — one half of the price — in exchange for payments under the table," it said.

To cover the losses, the employees asked the bank for advances although the store's business loan agreement allowed only the Wards to authorize advances, it said. "The employees used this money to hide the losses that the dealerships were taking on the discounted sales," the decision said.

By the time the Wards discovered the alleged scheme in 2018, they owed the bank about \$2.8 million for the double-booked loans, the court said. As part of a 2020 loan refinancing, Ward Chrysler signed a \$2,573,874 promissory note the Wards personally guaranteed, the

see LAWSUIT, Page 16

F&I DATA

Average interest rate increases to 11.7% for used-vehicle loans

Car shoppers in the 1st quarter of 2024 financed an average of \$27,774 on used vehicles, down \$836, or 2.9%, compared with a year earlier, according to Edmunds.

But used-vehicle monthly payments held steady, down \$5 to \$546, as the average interest rate on used models rose to 11.7%.

The average new-vehicle interest rate was 7.1% during the quarter. Edmunds said its analysts encouraged consumers to watch incentives on certified pre-owned vehicles "since used-vehicle interest rates are particularly high."

| | Q1 2024 | Q4 2023 | Q1 2023 |
|--|----------|----------|----------|
| Average used-vehicle loan term (months) | 69.7 | 69.9 | 70 |
| Average used-vehicle monthly payment | \$546 | \$561 | \$551 |
| Average amount financed on used vehicles | \$27,774 | \$28,643 | \$28,610 |
| Average used-vehicle interest rate | 11.7% | 11.6% | 11.1% |
| Average used-vehicle down payment | \$4,133 | \$4,122 | \$3,999 |

Source: Edmunds



We Are Deep-Rooted

We ensure our clients are confident and secure about their future. iA American has the unique ability to make long-term decisions that help you reach your goals, standing by your side every step of the way.

iaawg.com | 1.800.346.6469

We are iA American.

iA
American
Warranty Group

Gates 000047

CAREGARD

continued from Page 14

is known as ALPHV, the agency said.

Gates said the stressful work environment following the breach took its toll, and he resigned for health reasons. But he said he also felt remaining with AFG would represent condoning secrecy about the incident.

"I feel like I have a duty to let people know," he said. "In my mind, this is a deliberate cover-up to try to get past not reporting."

Safeguards Rule

The Safeguards Rule has required since 2003 that dealerships and other "financial institutions" protect customer information. In 2021, the FTC demanded businesses enact specific practices by Dec. 9, 2022, to support that protection; it later extended the compliance deadline to June 9, 2023.

The Safeguards Rule before its current iteration already required financial institutions to use "service providers that are capable of maintaining appropriate safeguards for the customer information at issue" and contractually compel those businesses "to implement and maintain such safeguards." The FTC has defined service providers broadly, describing them as any vendor that "receives, maintains, processes, or otherwise is permitted access to customer information."

The updated rule adds a requirement that dealerships and financial institutions periodically review those vendors "based on the risk they present and the continued adequacy of their safeguards."

Gates alleged CareGard wasn't ready for either the FTC deadline or the breach. Though the auto retail industry faced the FTC's June 9 deadline, Southeast Toyota allowed CareGard a "grace period" of extra months to meet the privacy obligations the distributor demanded, according to Gates.

Southeast Toyota said it had reached

out to CareGard after being contacted for this report by Automotive News and was told none of its data was affected.

"SET is not aware of any data incident CareGard experienced that impacted SET's data or would have required CareGard to provide notice to SET," Southeast Toyota said in a statement.

Southeast Toyota provided no response to an inquiry about Gates' account of an extended deadline.

Gates also alleged AFG over time had cut Integris' IT role "down to just monitoring." At the time of the breach, CareGard's IT had been delegated to a claims manager who was not a technology specialist, he said.

Integris "found the ransomware and alerted CareGard, but they couldn't do anything about it," Gates said. CareGard said in its statement that Integris "promptly restricted access to our network immediately" upon alerting CareGard on Aug. 13.

AFG and CareGard had no incident response plan when the breach occurred, Gates alleges.

"For years prior to this incident, CareGard has maintained both internal IT personnel as well as third-party cybersecurity service company support," CareGard said in its follow-up statement.

'Reporting requirements'

Booz Allen Hamilton, which was assigned by an AFG insurer, asked AFG to save the firewall and virtual private network logs, according to Gates. However, the claims manager had reset the firewall and server following the breach — which inadvertently erased access records and details on which files were compromised, Gates said. That outcome wasn't intentional; the manager simply didn't know any better, he said. The manager did not respond to messages from Automotive News seeking comment.

On Aug. 17, CareGard CFO Amanda Tettleton told Brewer, Gates and others

Safeguards Rule updates

The Federal Trade Commission's Safeguards Rule is meant to protect consumer information used by auto dealerships and other "financial institutions." Here are 9 key provisions of the updated Safeguards Rule that took effect June 9. The provisions require the institutions to:

1. Select a qualified person (either an internal expert or expert contractor supervised internally) to oversee security.
2. Have that expert report to a board or a senior officer.
3. Develop an information security risk assessment.
4. Create a plan to control those risks.
5. Have a plan for responding to a "security event" such as a breach.
6. Regularly monitor or test the system.
7. Train staff.
8. Use service providers that can secure information, contractually mandate they do so and periodically review their risk and security precautions.
9. Adapt the security program as needed so it stays current.

Upcoming addition: Starting May 13, businesses that find an unauthorized party has acquired unencrypted information on at least 500 consumers must notify the FTC no later than 30 days after discovery of the access.

that 105,910 files had been encrypted and provided a summary of their contents, according to an email provided by Gates. She did not identify which third-party companies and customers were affected, but her assessment did mention hundreds of QuickBooks records and claims files.

Later that day, AFG consultant Shawn Lucas wrote to Brewer, Tettleton, CareGard Chief Revenue Officer Keith Cooper and Gates: "There are several reporting requirements with respect to data breaches and ransomware," according to another email provided by Gates. Lucas wrote that required notifications included the local FBI branch; any "employees, contractors, agents, customers and/or dealers" whose information was exposed; and "Dealers, Nissan, SET, Genuine Lifetime, MBUSA, etc.," because "if information that exposes their customers was breached there is a requirement in most cases."

In October, the FTC would announce a Safeguards Rule amendment demanding financial institutions tell the agency about any breaches

where the threat actor acquired unencrypted information on at least 500 customers. That mandate takes effect May 13.

On Aug. 21 of last year, Tettleton called a meeting to discuss whether AFG should communicate with Blackcat, according to another email provided by Gates. According to Gates, this communication — which he said could have discovered the extent of the breach — never happened, despite being recommended by Booz Allen Hamilton.

CareGard said it "replaced all computers, firewalls, network switches, Wi-Fi routers, and anything else that was network related" in response to the breach.

"We also fully engaged Integris to extend our coverage and harden our systems and security to further ensure this will not happen again," it said in the statement. "Since then, Integris has remained fully engaged, and we work closely with them to ensure we are doing everything possible to eliminate future threats."

Integris told Automotive News it was

looking into a request for clarification on its role in the breach response but did not respond by press time.

A final report?

Booz Allen Hamilton ended its investigation Sept. 18, according to Gates. On Oct. 30, Lucas asked whether Booz Allen Hamilton had provided a final report, according to another email Gates provided.

"Did they determine how many customers were affected?" Lucas wrote, and said he was thinking about "regulatory compliance and SOC 2 final audit prep," in reference to Service Organization Controls 2 auditing, which looks at a company's security processes.

"I am not aware and have not seen a final report from Booz Allen," Gates wrote in the packet of documents he provided Automotive News. "I find this to be extremely troubling."

Brewer, in an Oct. 31 email provided by Gates, told Tettleton to send him the report from Booz Allen Hamilton, but in another communicate that day told Lucas: "We will not be receiving a formal legal report. This is not customary for obvious [reasons]. Who said we needed it. Why are you asking?"

As of press time, Booz Allen Hamilton had not responded to a request from Automotive News for clarification on its role in the breach response and the existence of a final report.

CareGard said it issued its statement in response to "recent email(s) received by some CareGard Dealers, Agents, and National Accounts concerning an alleged 'ransomware data breach.'" It was unclear which other parties besides Automotive News, if any, had received the statement.

"There are a lot of deals, business deals and a lot of clients that are relying on the premonition that CareGard and ... subsidiaries are handling their data properly, and have made commitments to CareGard, and CareGard has never let them know," Gates said. "They just act like nothing ever happened."

LAWSUIT

continued from Page 14

court said.

The Wards and the Chrysler dealership sued the Bank of Herrin for breach of contract, negligent misrepresentation, racketeering and consumer fraud violations. They alleged in the suit the bank knew about the scheme by June 2018

"and knowingly issued loans for which it had no collateral. Instead of revealing this information to the Wards, the bank made a conscious and deliberate decision to join the scheme."

The suit alleges the bank backdated the double-booked loans and failed to disclose to the Wards certain vehicles weren't physically present on the store's lots during inspections. In addition, it said the bank was "well aware" it was ap-

proving loans for up to 75 vehicles at a time but didn't tell that to the Wards during negotiations on new loans and guarantees.

According to an affidavit by Mark Ward, he discovered a problem with the inventory in December 2018 "when he was informed about missing cars from the used car lots, cars for which they had borrowed money to purchase but were no longer present to sell to pay back the borrowed money."

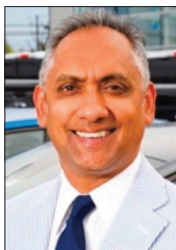
The Appellate Court's March 20 ruling upheld a lower court order barring the bank from seizing collateral while the litigation continues. The court accepted the Wards' argument that allowing the seizure of assets would cause them "irreparable harm." A spokesperson for the dealership's law firm declined to comment on the case. The bank's lawyer didn't respond to multiple messages from Automotive News.

Automotive News

People on the Move

See listings and post your own:
autonews.com/people

DIVERSITY IN DEALERSHIPS



ALL-STAR OF THE WEEK
Santosh Viswanathan
CEO, Lakeshore Chrysler
Dodge Jeep Ram, Seaford, DE
Stellantis
Seaford, Delaware

STELLANTIS
DEALER DIVERSITY

Meet Santosh Viswanathan, a principled business strategist whose philanthropic activities include supporting local food banks and domestic violence shelters led to a nomination for TIME Dealer of the Year. Make a difference in your community, join the Stellantis Dealer Network. Visit MinorityDealers.com or email DealerDiversity@Stellantis.com for more information on partnering with or mentoring minority dealer candidates.

AUTOMOTIVE



NEW HIRE
Dan Boxeth
Vice President of Engineering
Inmotive
Toronto, Ontario

Inmotive

Dan Boxeth has been named Inmotive's vice president of Engineering, following 31 years of working for Ford Motor Company, most recently serving as chief technical officer on several programs. He has substantial experience in technical project management, leading cross-functional teams and launching new vehicles and technologies. He earned a bachelor's degree and a master's degree in mechanical engineering from Rose-Hulman Institute of Technology and the University of Michigan, respectively.

AUTO DEALERSHIP SALES, MERGERS AND ACQUISITIONS



NEW HIRE
Adam Scott
Partner, Texas & Midwest Office
Performance Brokerage Services, Inc.
Austin, Texas

Performance
BROKERAGE SERVICES

We are proud to welcome Adam Scott as Partner in our Texas & Midwest Office. A graduate of Texas Tech University, Adam has amassed over 25 years of experience in automotive retail with Ford, General Motors and Nissan. He served as Group 1 Automotive's Twenty Group Chair and received multiple awards during his tenure in executive management. Adam's broad understanding of dealership operations coupled with first-class customer service gives him specialized knowledge and expertise for his clients.