A widespread breakdown in security safeguards at Equifax Inc. aided hackers as they broke into the company’s systems and gained access to personal information of millions of Americans, according to prepared testimony former CEO Richard Smith plans to deliver Tuesday.

The mishaps detailed in Mr. Smith’s testimony point to a range of weaknesses in the measures taken to protect consumer data at one of the largest credit-reporting firms in the U.S. They included staffers not responding properly to a public warning in early March about a vulnerability in software the company was using and a malfunctioning scanning tool that failed to identify the threat.

As a result, Equifax for months was unaware that it was vulnerable and that hackers were ransacking its systems. The company didn’t detect suspicious activity until July 29.

“The breach occurred because of both human error and technology failures,” Mr. Smith is expected to say in testimony Tuesday before a subcommittee of the House Committee on Energy and Commerce.

Equifax said separately Monday that a review into the hack has now been completed. It increased the number of affected U.S. consumers by 2.5 million to 145.5 million.

Mr. Smith’s testimony Tuesday will be the first of at least three scheduled appearances on Capitol Hill this week. He is also due to testify Wednesday before the Senate Banking Committee and on Thursday before the House Financial Services Committee. Mr. Smith last week stepped aside as Equifax’s chairman and CEO.

Legislators are expected to press Mr. Smith for more details about the circumstances leading up to the hack and the company’s response to it. Another area of concern: which executives were aware of the breach and when, especially given share sales by three top executives days after the company discovered the hack.
Beyond the security breakdown, the testimony highlights how the company's external declarations about its security were at odds with what was happening inside the company. Mr. Smith and the company made comments in the weeks after the breach was discovered about Equifax's commitment to security. Equifax had notified the Federal Bureau of Investigation of the breach on Aug. 2 and also had brought in FireEye Inc.'s cyber-investigations division Mandiant to investigate the hack.

The security breakdowns stem from an early-March warning to Equifax and other companies of the need to patch a vulnerability in software called Apache Struts. A day later, Equifax emailed that notice to its information-technology personnel asking for the software to be upgraded.

Although the company's patching policy required a fix within 48 hours, the vulnerable version of Apache Struts within Equifax wasn't identified or patched in response, according to Mr. Smith's testimony. Later that month, the company's information-security department ran scans that should have found systems vulnerable to the Apache Struts issue. The scans failed to do so.

After the company's security staff noticed suspicious traffic on July 29, information about the breach moved slowly between some in senior leadership. Mr. Smith said that the company's then-chief information officer informed him of suspicious activity on July 31. Mr. Smith didn't have an indication of the scope of the attack or know that consumers' personal information had been stolen, according to his testimony.

Mr. Smith's testimony said that he only found out on Aug. 15 that consumers' personal information had "likely" been stolen. Two days later, Mr. Smith gave a roughly 40-minute presentation and took questions at a breakfast meeting at the University of Georgia's Terry College of Business.

During that event, he praised the rapid rate at which the company expanded under his leadership and spoke about the threat of data fraud. That same day, according to Mr. Smith's testimony, he held a senior leadership meeting where he learned that large volumes of consumer data had been compromised in the breach.

The company's board didn't know about the breach at the time. Instead, Mr. Smith says in his testimony that he notified Mark Feidler, the board's lead director, on Aug. 22. Equifax last week named Mr. Feidler the board's nonexecutive chairman after Mr. Smith stepped down.

Mr. Smith says that on Aug. 22 he also notified his "direct reports" who ran various business units about the problem. Mr. Smith doesn't state which executives found out about the breach that day. Three of his top deputies, including finance chief John Gamble, sold shares on Aug. 1 and Aug. 2. The company has said the executives weren't aware of the breach at the time.

Equifax's full board found out about the breach on Aug. 24 and 25, almost a month after it was first detected. A board meeting took place on Sept. 1 where the scale of the breach and remediation efforts were discussed. Three days later, the investigative team had a list of approximately 143 million consumers whose personal information had likely been stolen.

The challenges didn't end there. As the company was trying to determine the scope of the breach, Mr. Smith's testimony says it was also working to set up a website to help consumers and to increase call-center staff.

Those efforts were riddled with problems in the wake of the public breach announcement on Sept. 7. That included a malfunctioning website and confusion over the legal rights of consumers who signed up for free monitoring. Mr. Smith's testimony says the "challenge proved overwhelming, and, regrettably, mistakes were made."

—Andrew Ackerman contributed to this article.
Write to AnnaMaria Andriotis at annamaria.andriotis@wsj.com and Michael Rapoport at Michael.Rapoport@wsj.com

Appeared in the October 3, 2017, print edition as ‘Equifax Ex-CEO Lays Out Lapses.’