Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

CFPB's 'Disturbing' Data Breach Sparks Ire, Credibility Doubts

By **Jon Hill**

Law360 (April 26, 2023, 12:10 AM EDT) -- A Consumer Financial Protection Bureau data breach involving sensitive information on dozens of financial institutions and potentially hundreds of thousands of their customers may damage the agency's credibility on data security and chill companies' responses to its information requests, financial services attorneys say.

The CFPB acknowledged last week that one of its examiners mishandled agency records by emailing them to a personal inbox, a breach that came to management's attention in mid-February and touched off an internal review that determined it to be a "major incident" the following month.

The unnamed examiner, who ultimately lost their job, was found to have forwarded confidential supervisory information on 45 financial institutions as well as more personalized customer information tied to seven institutions, including names and certain other data related to 256,000 consumer accounts at one firm.

Although the CFPB has said it is "taking appropriate action to address this incident," Republican lawmakers were still waiting as of Monday for the agency to provide briefings they had requested on what exactly went wrong and how the situation is being handled.

Some financial services attorneys are also raising concerns about what they see as a troubling lack of transparency surrounding the breach, which appears to have taken more than two months for the CFPB to publicly acknowledge — and only after the Wall Street Journal first broke the story.

"No private company would be allowed to behave like this," said Scott Pearson, leader of Manatt Phelps & Phillips LLP's consumer financial services practice. "That's what's so disturbing about this. You are seeing a double standard."

"I think it's a tremendous blow to the credibility of the bureau," Pearson added.

"More Questions Than Answers"

The CFPB has framed the breach as serious but still limited in scope. Of the sensitive material forwarded by the examiner, for example, the agency has said the consumer-linked data was found overwhelmingly in just two spreadsheets and doesn't appear to have gone further than the staffer's personal inbox.

The CFPB has also defended its handling of the incident as by the book, maintaining that it alerted the

proper oversight authorities once it realized what had happened and has since reached out to affected financial institutions as well.

But Pearson and other financial services attorneys see a number of unanswered questions about the breach that give them pause, including why the CFPB's networks weren't better locked down to prevent an unauthorized transfer of documents in the first place.

It's not uncommon, for example, for companies to augment their email systems with so-called data loss prevention tools that scan outgoing messages and block those found to contain sensitive material.

The examiner, however, was apparently able to send dozens of emails containing confidential data without being thwarted or detected. In fact, the breach seems to have been discovered almost by accident. A co-worker spotted that the examiner had copied a personal email address on some correspondence, according to the CFPB.

"Everyone has data breaches. That's just the nature of the beast," said Nathan Taylor, a financial privacy partner at Morrison & Foerster LLP. "But one of the inferences here is that [the CFPB's] controls may not have been as robust as one would expect for handling such sensitive data."

And if one examiner was able to slip past the CFPB's data security safeguards, Taylor said it begs the question of whether this kind of improper personal email use is a more widespread phenomenon within the agency's ranks.

"Was this a solitary event, or could this be sort of the first peel of the onion?" Taylor said. "There are more questions than answers right now."

No cybersecurity measure is perfect, of course, and mistakes do happen. But with the CFPB increasingly asserting itself on data security and privacy issues in consumer finance, the breach's disclosure is being met with more than a whiff of schadenfreude in some quarters.

It was only last summer, for example, that the CFPB put out guidance warning financial companies that lax data security could qualify as an unlawful, unfair practice and expose them to potential liability.

The breach also comes at a time when tensions between the CFPB and the financial industry have been running particularly high, with companies viewing the agency as overly eager to find fault and flex its regulatory muscles.

"The reality is that data security is challenging for everyone," Manatt's Pearson said. "But the fact that this happened at the bureau illustrates that perhaps we shouldn't be acting like everyone is strictly liable for everything and perhaps ought to be a little more understanding of what the real world is like."

"That's not how we see the bureau behaving," Pearson added.

Feeling the Squeeze

There are several ways the breach could turn into more of a lasting headache for the CFPB.

For one, some attorneys told Law360 that it could aggravate companies' wariness in responding to CFPB civil investigative demands unless they are given greater assurances regarding the agency's ability to

protect any sensitive data they may turn over about themselves or their customers.

Nevertheless, a company in this situation can't hold out forever, as the CFPB can always sue to compel compliance. But that process is neither quick nor a guaranteed win for the agency, and even if it chooses to narrow its demand instead of going to court, the negotiations could still add time-consuming friction.

"I've had people tell me they would not give the CFPB a shred of data until they produce a remediation report," said Joann Needleman, leader of Clark Hill PLC's financial services regulatory and compliance practice. "And I think a judge could be sympathetic to that request."

"If the matter ended up in court, a defendant wouldn't be challenging the bureau's structure or the CFPB's right to ask for the information," Needleman added. "But financial institutions do have a duty to their customers and to protect their information. The bureau has a duty to those same customers and to protect them from something like this happening."

The breach could similarly complicate the CFPB's ability to conduct the kind of sweeping, marketwide "inquiries" that the agency's director, Rohit Chopra, has used to scrutinize issues such as the explosion of buy-now, pay-later financing and Big Tech's expansion into payments.

Those inquiries have relied on a different subpoena-like authority that allows the CFPB to grill companies for "market-monitoring" purposes, but this authority has murkier boundaries that some firms might now feel more justified in testing on data security grounds.

Whether the CFPB might have to compensate anyone for the breach also remains to be seen. When asked Friday if the agency will pay for credit monitoring for affected consumers, a spokesperson told Law360 only that the CFPB is working with affected institutions to "determine additional steps that may be necessary."

Confidential supervisory information is typically considered property of the government, Morrison Foerster's Taylor noted, so affected financial institutions wouldn't have much of a claim there. As for personal information involved in the breach, Taylor said much will depend on behind-the-scenes judgments about how much potential there is for consumer harm.

Compared to the fingerprints, Social Security numbers and other identity details leaked in the government's massive 2015 personnel records breach, for example, the names and "transaction-specific" account numbers reportedly contained in spreadsheets forwarded by the examiner look to be lower stakes.

"I would argue credit monitoring doesn't sound relevant there," Taylor said, adding that just notifying affected consumers could be tricky enough on its own and may not be feasible for the CFPB to do itself without requesting additional contact information. "That creates this quandary if you're one of the financial institutions at issue here ... Do you feel good about giving the CFPB more data about your customers?"

But even if no cleanup costs materialize, the bureau may still have to pay a political price. Republican lawmakers have already seized on the incident as a manifestation of what they see as the CFPB's lack of accountability, setting up more fodder for potentially bruising congressional oversight hearings and investigation.

The CFPB "has become a very political agency, and, you know, turnabout is fair play," Pearson said. "I think you're going to see a lot of criticism of the bureau's double standard, particularly in Congress."

Will It Blow Over?

The CFPB, for its part, has said that companies need not fear for the safety of their data in its hands.

"The CFPB maintains a comprehensive cybersecurity program to safeguard its systems and the data maintained on those systems," a spokesperson told Law360 on Friday, adding that the program meets federal standards and has achieved an audit rating that "represents an effective level of security."

In the wake of the breach, the CFPB is also "examining current information security practices, adopting technical solutions, and expanding insider threat measures to provide additional tools to help strengthen data protections," the spokesperson said.

Not all financial services attorneys are persuaded that the breach will actually turn out to be more than a temporary embarrassment for the agency.

When it comes to interacting with the CFPB, the calculus about how much information to share may not meaningfully change for many financial institutions, according to Allison Schoenthal, a Goodwin Procter LLP partner and co-chair of the firm's banking and consumer financial services practice.

"Our financial institution clients are extremely sensitive about any information that leaves their institution," Schoenthal said. "Data security and protection of customer information are top of mind for everyone."

Schoenthal added that she has also found the CFPB to be fairly accommodating in that regard. In her own experience, she said, the agency's examiners "have been pretty reasonable about taking less [information] to give greater security and comfort."

Taylor of Morrison Foerster similarly said that while the breach may underscore the reasons why a company wouldn't be eager to hand over reams of data to the CFPB, he doubts it will provide real ammunition to those looking to resist investigative demands or dissuade the agency from dialing up the heat on others' data security practices.

And to the extent that the breach could fan the flames of opposition to the CFPB on Capitol Hill, Taylor noted that it was already a "pretty robust fire to begin with."

"Is the CFPB potentially red-faced for a time based on the incident? Sure," Taylor said. "But I don't think it materially changes anything."

The wild card is what further investigation of the breach could find. The CFPB has referred the matter to its Office of Inspector General, and it's likely that Republicans will also seek to dig into what happened.

If there's any hint that the incident was worse than advertised, mishandled or part of a more systemic problem, it's not hard to imagine a fresh scandal erupting that would be much harder for the agency to shake off.

"The fact that there wasn't any public word of this [breach] until pretty recently is shocking enough,"

Manatt's Pearson said. "If a big bank did this, I guarantee you there would be horrific press releases out there talking about how terrible the bank is, how awful its executives are, and how they are hurting all of their customers."

"So the idea that this agency wouldn't be subjected to all of that when they engage in the kind of conduct that they would rip companies apart for is really bothersome to me," he said.

--Editing by Jill Coffey and Jay Jackson Jr.
