Shumaker

NOVEMBER 17, 2026 | PUBLICATION

Client Alert: When the Mail Stops: What the Bankruptcy Noticing Center Outage Teaches Creditors About Court Technology and Data Risk

Every bank and credit union in Florida knows what a regulator asks when a critical vendor goes down: what was your backup, and who knew? In October 2026, the federal bankruptcy courts faced that question themselves. A cybersecurity incident at the contractor that sends every federal bankruptcy notice took the system offline for about two and a half weeks. For Florida lenders, servicers, and collectors, the fallout is still working its way through their accounts.

INDUSTRY SECTOR

Technology

SERVICE LINE

Artificial Intelligence
Bankruptcy, Insolvency & Creditors' Rights
Cybersecurity
Data Privacy
Technology

RELATED PROFESSIONALS

Elizabeth R. Brusa

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

What the BNC Is

The Bankruptcy Noticing Center, or BNC, is the system that prints, mails, and emails the official paperwork in every federal bankruptcy case in the country. It is operated for the federal judiciary by BAE Systems, a defense and technology contractor. Many creditors without counsel in each case rely on it alone.

What Happened

Most courts date the disruption to October 9, 2026, although sound courts place it as early as October 7. On October 15, the Administrative Office of the U.S. Courts confirmed a cybersecurity incident affecting BAE's systems. Paper and email notices stopped nationwide. In late October, the Judicial Conference declared a nationwide "Bankruptcy Rules Emergency," giving judges broad power to extend or toll deadlines through

January 7, 2027. Service resumed October 26. Notices caught in the backlog were stamped with a warning that they "may have been sent later than intended."

What Florida's Courts Required

Florida's three bankruptcy courts each took a different approach. The Middle District shifted the burden to debtors, requiring them to serve the notice of case filing on all creditors within three days. It extended certain deadlines by 60 days in cases filed on or after October 7. Parties harmed by missing notice could seek relief by explaining how it affected them. On October 27, the court ended those orders and replaced them with one addressing post-outage issues.

The Southern District adopted emergency procedures under Administrative Order 2026-06 and ended them under Administrative Order 2026-07 once service returned. The Northern District went further. It assigned new service and noticing responsibilities under Administrative Order 26-004 and specifically urged creditors to read it. The court later retired those procedures but preserved any service properly made during the outage.

In practice, a lender with cases in Orlando, Miami, and Tallahassee faced three sets of rules at once. Best practices require creditors to calendar both original and extended deadlines, and keep records of what you received and when, because relief for a missed deadline generally requires showing actual harm.

Florida Collection Exposure

A bankruptcy filing freezes collection activities immediately, and the law does not wait for the mail to catch up. Under the Bankruptcy Code, an individual debtor harmed by a willful stay violation can recover actual damages, including attorneys' fees, and in some cases punitive damages (11 U.S.C. § 362(k)). Damages generally depend on whether the creditor knew of the case. The outage may help explain early missteps, but that defense ends once a customer, a lawyer, or the docket provides notice.

Florida adds a second layer. The Florida Consumer Collection Practices Act applies to any person collecting a consumer debt, including original creditors, not just third-party collectors. It prohibits asserting a legal right the collector knows does not exist (Fla. Stat. § 559.72(9)). Remedies include actual damages, up to $1,000 in statutory damages, attorneys' fees, and punitive damages in appropriate cases (Fla. Stat. § 559.77). If your team took any collection steps on a Florida consumer account after October 7, confirm that the customer had not filed for bankruptcy first.

Data Privacy and the Vendor Risk Lesson

According to a BAE spokesperson quoted by BleepingComputer, the incident was confined to the BNC, and no personal information was compromised. To date, the cause has not been made public, and whether any data was accessed remains an open question. That matters, because bankruptcy notices carry names, home addresses, account information, and evidence of financial distress, and the BNC maintains creditor contact data on a national scale.

The incident also follows a pattern. In August 2025, the Administrative Office acknowledged a series of serious, ongoing attacks on the courts' electronic filing system and added safeguards for sealed records. Earlier that year, Judge Michael Scudder, who chairs the Judicial Conference's technology committee, told Congress that the system and its public-access counterpart had become too vulnerable to keep and needed to be replaced. The BNC disruption, caused by a single contractor, BAE, which handles work most people never think about, turned out to be a single point of failure for every bankruptcy case in the country. An

ordinary IT contract had quietly become critical to due process.

Financial institutions would recognize this risk immediately. Under the 2023 interagency guidance from federal banking regulators, a bank that outsources a critical activity remains fully responsible for it. The bank must vet the vendor, negotiate contract protections, monitor performance continuously, and plan for failure. In the event of a vendor outage, disruption, or breach, examiners would ask about backup systems, incident reporting, and what data the vendor held. The public record does not answer those questions for the courts. Bankers are held to that standard for a mortgage servicing platform and productions from other vendors; the court system that delivers legally required notice deserves no less.

Key Takeaways and Reminders from the BNC Outage

Treat the docket as the official record. Treat a notice in your mailbox as a courtesy copy. If your business holds meaningful bankruptcy exposure, pair the court's notices with an independent monitoring source that draws directly from court records so that an outage cannot leave you uninformed.

Protect against automatic stay violations. Before repossessing, garnishing, or sending a demand, run a bankruptcy search on the account. A collection action taken against a debtor in bankruptcy can expose you to sanctions, even if you never received notice from the BNC. In Florida, the same misstep can also support a claim under the state's consumer collection law, so build a bankruptcy check into collections workflows rather than relying on staff to catch it.

For the BNC outage period, do not process late notices as routine. Mail that arrived after October 26 may describe hearings or deadlines that have already passed. Keep a written record of when each notice arrived and what you did about it. That record is what a court will want to see if you ask for relief.

Apply your vendor risk program to your own noticing chain. If outside vendors receive, store, or act on bankruptcy notices for you, confirm how they handle outages and protect the data they hold. Map the full chain, including servicers, collection agencies, monitoring services, and outside counsel, and ask whether any of them depends on a single source for bankruptcy information.

Put outage protections in writing. Federal banking guidance describes contract terms worth having with critical vendors, including audit rights, limits on how the vendor uses and shares your customers' information, security requirements for personal data, and oversight of the vendor's own subcontractors. Add a firm deadline for telling you about a security incident and a right to exit if the vendor falls short.

Test the backup plan before you need it. Regulators describe operational resilience as the ability to keep critical operations running through any disruption, and they expect financial services businesses to decide in advance how much disruption they can tolerate. Run a short exercise that asks a simple question: if court notices stopped tomorrow, how would we know, and who would act?

For regulated financial services businesses, be ready for the examiner's questions. Regulation guidance does not create new rules, but examiners use it to judge how well an institution manages its vendors. Document what your team did during the outage, which accounts it checked, and what it changed afterward.

Fintechs and payment processors: expect your bank partners to ask. Regulation guidance calls out fintech relationships, including merchant payment processing. A bank partner that is reviewing its own bankruptcy notice controls will likely ask how yours worked during the outage. Have a clear answer ready.

Closing Thought

Banks, credit unions, fintechs, lenders, and payment processors already live in a world where every critical system has a backup plan, and every important vendor gets a hard look. The BNC outage is a reminder that the courts are part of that world too. Court technology is now one more link in the chain that carries the information your business depends on, and that link deserves the same attention as your core processor or your servicing platform. As regulators keep raising expectations for resilience and vendor oversight, the institutions best positioned are the ones that treat bankruptcy noticing as part of their own operations, not something that happens somewhere else. The next disruption is a question of when, not if. The businesses that plan for it now will be the ones that keep moving when it comes.

© 2026 Shumaker, Loop & Kendrick, LLP. All Rights Reserved. Privacy Policy/Disclaimer

Shumaker