New Jersey Courts
Independence • Integrity • Fairness • Quality Service

Administrative Office of the Courts

**GLENN A. GRANT**
Administrative Director of the Courts

Richard J. Hughes Justice Complex • P.O. Box 037 • Trenton, NJ 08625-0037 njcourts.gov • Tel: 609-376-3000 • Fax: 609-376-3002

**DIRECTIVE #11-23**

**TO:** **Hon. Thomas W. Sumners, Jr.**
**Assignment Judges**
**Hon. Mala Sundar**
**AOC Directors and Assistant Directors**
**Clerks of Court**
**Trial Court Administrators**

**FROM:** **Glenn A. Grant, Administrative Director**

**SUBJ:** **Responding to Information Security Incidents, Including Compromised Attorney Accounts**

**DATE:** **June 26, 2023**

---

Cyberthreats are of growing concern in all areas of society. Government agencies, court systems, law firms, and individual attorneys face threats to information security on an ongoing basis, with some of those resulting in compromises or breaches that have the potential to harm not only the affected entity but others with whom that entity communicates.

Consistent with Rule 1:32-2A ("Electronic Court Systems, Electronic Records, Electronic Signatures, Metadata, Cybersecurity"), this directive formalizes the steps already being taken by the Judiciary to identify and respond to at-risk or compromised accounts of users of court systems. It also outlines the process for an external user to notify the Judiciary if the user becomes aware that an individual or firm account may have been compromised. The Judiciary will maintain the confidentiality of all information shared as part of reporting and responding to a cybersecurity incident, whether identified by the Judiciary or reported by a court user.

## Existing Judiciary Safeguards

The Judiciary has implemented an array of interlocking steps to protect against cybersecurity threats. Those strategies include multiple automated processes[1] to scan and screen incoming communications, including emails and electronic filings, and blocking of transmissions identified as potentially harmful. Such protections are designed to prevent against any harm to Judiciary systems as well as any perpetuation of harm via further transmission of a compromised communication.

## Judiciary Identification of and Response to Security Risks

As a result of existing safeguards, the Judiciary often identifies a potential security breach before the court user is aware that the user's account has been compromised. When this occurs, the Judiciary implements precautionary measures, including to block any incoming emails from the user and to temporarily disable the user's accounts[2], including capacity to log into eCourts. Those safeguards continue pending confirmation that any threat has been resolved.

Consistent with longstanding and current practice, the Judiciary will continue to promptly notify a court user that steps have been taken to isolate and preempt electronic transmissions based on a potential security risk. Such notice will include information about any steps required to resume uninterrupted access to Judiciary systems. To the extent possible, the Judiciary also will provide its best estimate about the timeframe for restoration of access to systems, as well as interim options to avoid unintended consequences as to pending and new matters.

---

[1] In addition to requiring users to complete two-factor authentication, incoming communications proceed through a web application firewall, or WAF. Transmittals then encounter a general firewall that identifies and protects against anomalous activity. All communications and filings are inspected for malware and suspected ransomware and are further scanned before receipt in a system. The Judiciary will continue to refine and enhance those security protocols consistent with information security standards.

[2] If an entire office or firm may have been compromised, the Judiciary may suspend all accounts at that office or firm.

## Responsibility to Inform the Judiciary of Known Security Issues

In some cases, an external court user may discover a potential or confirmed cybersecurity breach before the Judiciary identifies the risk. An attorney or other user of Judiciary electronic systems who becomes aware of such a cybersecurity incident should promptly notify the Judiciary by calling the Superior Court Clerk's Office at (609) 421-6100. Email, including personal email, should not be used to provide notice because of the possibility that an email communication might inadvertently contain and thereby transmit malware or ransomware.

Once notified that a court user account may have been compromised, the Judiciary will take appropriate steps to investigate the potential risk, safeguard court systems, and protect other court users. Such steps may include quarantining and blocking further transmissions from the potentially compromised account(s) and temporarily suspending access to Judiciary systems. Again, the Judiciary will work with the court user to restore system access once the threat has been resolved.

Additional information may be requested from the court user in order to investigate and respond to the cybersecurity incident. The Judiciary as always will maintain the confidentiality of any such information shared by the court user and will collaborate on any interim options, such as a new temporary account, to minimize potential harms to clients and others.

## Questions

Questions regarding this Directive should be directed to the Superior Court Clerk's Office at (609) 421-6100.

cc: Chief Justice Stuart Rabner
Steven D. Bonville, Chief of Staff
Jack McCarthy III, CIO
Meryl G. Nadler, Counsel to the Admin. Director
Special Assistants to the Admin. Director
Sajed Naseem, CISO
IT Division Managers