Bottomline

Delaware Criminal Justice Information System

Keeping Sensitive Information Protected from Misuse by Authorized Users

DELAWARE CRIMINAL JUSTICE INFORMATION SYSTEM

DELJIS
SERVING THOSE WHO SERVE OTHERS

Customer Overview

Delaware Criminal Justice Information System (DELJIS). Delaware was the first US state to implement an integrated Criminal Justice Information System (CJIS) that supports electronic sharing of information within the criminal justice community. While the DELJIS has been in existence since 1990, it is constantly changing to meet the needs of system participants, including State and local police, the Attorney General's Office, the Public Defender's Office, the Courts, and the Department of Corrections.

Key Features:

- Provides full visibility into user actions, deterring abuse
- Supports compliance of Delaware laws relating to access and dissemination of records
- Real-time alerts detect security breaches immediately, increasing officer safety
- Recorded data is encrypted and digitally signed, meeting forensic evidence requirements

THE CHALLENGE

The DELJIS agency facilitates the electronic sharing of information among all participating agencies, including case information from initial contact to case-closing events (i.e. arrest data, motor vehicle and license data, crime incident data). Over 7,000 authorized users are able to determine the status of a case instantly, which enhances the ability to process criminal cases efficiently. Law enforcement's instant access to criminal history, warrant, and protection order information has been a critical component of the department's success. Public safety has been greatly enhanced by the efficient exchange of such background information.

The system is based on a central mainframe platform which provides several types of user interfaces. These interfaces include secured web access for law enforcement officers, enabling them access to the system from their patrol cars. Access to CJIS is protected by standard security tools which grant access only to authorized end-users. However, these tools do not monitor how end-users utilize their authorized access and cannot detect or prevent misuse by the authorized end-users.

Various types of authorized end-users may pose potential threats to the system, for example:

- A disgruntled employee with easy access to confidential data
- An employee looking to harm someone by disclosing information
- An employee seeking financial gain by selling sensitive information

The information maintained by CJIS is highly sensitive, and there are many cases that require the ability to reconstruct user actions in order to find what specific data was accessed by a specific user. In addition, it is necessary to know, beyond a "reasonable doubt," that no one else would have accessed the same information within the timeframe in question.

If an incident needed investigation, the investigation team had to plow through mountains of paper logs. Depending on the type of search requested, one second of case activity could be represented by one box full of paper. The investigation process had significant shortcomings. It was manual and labor intensive, left room for error and had a long turnaround time.

As a result, requests for investigating activity logs were honored only for major crimes, and not for other suspicious cases.

Bottomline

SEARCHING FOR A NEW SOLUTION

The Secretary of the Department of Technology and Information and CIO for the State of Delaware, Thomas Jarrett, recognized the critical situation DELJIS was facing and searched for a solution. The desired solution needed to meet the following goals:

- Reduce the overall time associated with investigations
- Have real time answers to questions of: Who? What? When?
- Ensure public and police safety by reducing the number of threats
- Assist Law Enforcement with criminal investigations of homicides and burglaries
- Set alerts to see if anyone accesses sensitive, case-related information

DELJIS turned to Bottomline Technologies and its Cyber Fraud and Risk Management Solution. The innovative solution was installed for evaluation. Within a few hours the system was up and running and started to record the activity of all end-users connected to the mainframe. The system reconstructs end-user sessions and allows investigators to quickly search for user sessions based on any field value that appeared in any user screen. Investigators can now visually replay user sessions, screen by screen. The evaluation installation was very successful and allowed DELJIS to meet its goals.

The patented technology tracks user behavior patterns at the application screen level and can build profiles of users and user-groups. The analytic engine generates alerts on suspicious events in real-time. An event may be considered suspicious if the current activity of an end-user is different from his normal behavior in the past, or if his behavior is different from his peers in the same department, or from peers with similar roles.

> *"The logging system performed fantastically better than expected. Turnaround time with the system was fabulous. Breach investigation time decreased by more than 90%." – P. Bell, Executive Director Delaware Criminal Justice Information System (DELJIS), the State of Delaware*

THE RESULTS

Bottomline's Cyber Fraud and Risk Management solution dramatically reduced the duration of internal investigations. For example, investigating 6 months of data now takes 20 minutes using the new solution, whereas it used to take 2½ months. And, it enables DELJIS to investigate every request from law enforcement agencies, not only major crimes.

In one example, an agency requested to check if any users accessed certain specific warrant information. A quick investigation using the Bottomline Cyber Fraud and Risk Management Solution revealed that a specific user accessed information on this warrant and disseminated it to an unauthorized person. This case resulted in one user arrest, one user terminated, and one user administratively reprimanded in addition to losing access to the system.

Learn how to detect and prevent fraud in your organization: ***5 Keys to Staying Ahead in a Fast-Moving Threat Environment***

READ REPORT

About Bottomline Technologies

Bottomline Technologies (NASDAQ: EPAY) helps make complex business payments simple, smart and secure. Corporations and banks rely on Bottomline for domestic and international payments, efficient cash management, automated workflows for payment processing and bill review, and state of the art fraud detection, behavioral analytics and regulatory compliance.

For more information, email info@bottomline.com or visit www.bottomline.com

Connect with us

bottomline.com

Corporate Headquarters
325 Corporate Drive,
Portsmouth, NH 03801,
United States of America

Phone: +1 603.436.0700
Toll-free: +1 800.243.2528
Fax: +1 603.436.0300
info@bottomline.com