edjuster
BY CRAWFORD & COMPANY

CONTENTS CLAIMS HANDLING AND THE **IMPORTANCE OF DATA PRIVACY**

60%
say the responsibility of protecting data rests with the company collecting the data

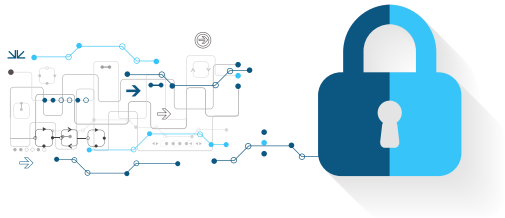
92%
agree companies must be proactive about data protection

77%
agreed with the statement that the digital world is creating new types and levels of risk for our business

65%
felt that there was not the proper level of investment to protect against these new digital risks

Source: PwC US Protect.me Survey, 2017

edjuster is North America's leading contents company, operating with a proprietary contents platform (exclaim/SaaS) that offers the capabilities required for effective management of Personally Identifiable Information (PII), while ensuring that client claims data is secure throughout the entire claims lifecycle.



An aspect of content claims that is often underestimated or overlooked is the importance of protecting customer data. As customer data is collected from the field or directly from customers over the phone, it can reside in multiple systems, which can present data security risks to insurers. It is critical that companies dealing with client data take the necessary steps to ensure that all customer data is adequately protected.

Protecting client data throughout the contents inventory process

edjuster's contents inventory process is conducted at client's homes or businesses and direct with policyholders over the phone. The company takes the following measures to guarantee that its content claims representatives protect client data throughout the claims inventory and valuation process:

- edjuster provides all employees with comprehensive continuing education & training for the management of personal client data
- edjuster's claims reps maintain a password-protected computer or mobile device
- It enforces screensaver password protection. If a computer is left unattended, a user must re-login before accessing the computer
- exclaim features a document management system that protects claim documentation, without requiring them to be on a local computer.

edjuster also takes data protection a step further, with ongoing investment in robust information technology infrastructure and a team of professionals to ensure client data is protected 24/7/365.

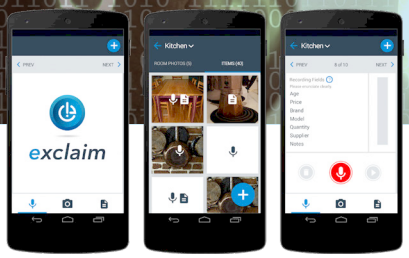
edjuster's IT mandate includes the following:

- Enforced screensaver password protection. If a computer is left unattended, a user must login to access the computer
- Employees must use a minimum password complexity on all corporate resources
- Two-factor authentication is mandated on all computer and phone devices
- Virus scanners that are constantly updated under centralized IT control
- e-xclaim includes a document management system that stores all personal information and claims related data in a secure environment
- Limited access to claim data and personal information through claim collaborators

How edjuster protects your data after claims have been completed:

Once on-site inventories have been completed, edjuster claims representatives are responsible for completing LKQ valuation using edjuster's proprietary and secure exclaim platform. In the unlikely situation an employee was to leave the company, the following steps are undertaken to ensure the utmost protection of all claims data:

- IT can remotely disable accounts, removing access to corporate email and other shared resources
- All employees use the corporate email system. When an employee departs, access to all resources are disabled
- The company's single-sign on capability disables the account in one place and access to email, corporate resources and exclaim are all simultaneously disabled
- Rep's telephones are controlled within a corporate policy, allowing remote deactivation and deletion of corporate assets from their telephone



The power of exclaim in protecting client data

The exclaim contents management platform offers a full featured, easy to use contents valuation and claims management solution delivered from the cloud as a Software-as-a-Service (SaaS). The system is designed to handle both high severity complex claims and the higher-volume, small claims – such as break and enter, theft losses.

Highlights of client data protection include:

- exclaim's mobile application is secured through the exclaim platform, as well as via phone device policies
- exclaim Mobile directly integrates with exclaim to upload the list of content items without having to offload to a separate spreadsheet or "print off" to send to the adjuster or other external source
- Policyholder and insurer information is available through the exclaim secure Mobile application which means that handwritten or printed information is no longer required
- Claims are securely managed in the cloud and are not downloaded to a computer or shared through non-secure means. Only claims reps with clearance are granted access to work directly on the claim within the application or browser

In addition to these data security policies and procedures, edjuster regularly complies with requests for security assessments with partners and insurers. The company has written policies that are traceable and tested, with documented results.

At a corporate level, edjuster ensures that all employees receive adequate levels of training with the handling of personal client data and information. All new employees receive initial training at hire with additional training provided on a regular basis.

Customer Portal and Policyholder Self-service Capability

edjuster enables policyholders to securely create contents claims list without having them complete paper statement of loss forms or via email. Instead we offer the following process:

- Secure link for policyholders
- Create contents list directly in the platform
- Upload completed content items directly into exclaim

Insurers using exclaim

Additional security features to comply with Insurer security protocols:

- Login access filtering; Restricts login to exclaim to a list of permitted locations specified by client companies. The locations are provided by your company's IT department and will be matched based on the IP Addresses that you are attempting to connect to exclaim. For example, if the organization only permits logging in from corporate and branch office locations then any attempt to connect to exclaim outside of those locations will be restricted.