



## Case Study – A Well-known e-Payment System Provider

**Assist an electronic payment system provider, display a watermark on employees' computer screens to remind them to handle confidential information with care.**

### Client Profile

This is a well-known electronic payment system provider based in Hong Kong.

### The Challenges

As a major electronic payment system provider in Hong Kong, the company deals with a large volume of transactional data on a daily basis. This data includes sensitive information such as payment details, payers, recipients, and other confidential data. Not only does this data involve sensitive business information, but it also involves the privacy of the payers.

To prevent employees from leaking confidential data, the company has implemented various measures. However, it is challenging to ensure that employees do not use their mobile phones to capture and share data displayed on their computer screens for the sake of convenience.

Moreover, due to some employees needing to work remotely, especially during the COVID pandemic, the company needs to find a solution to further remind employees to handle the content displayed on their screens carefully when dealing with confidential data. They should not casually capture and share it using their mobile phones.

### The Solution

Ultimately, the company chose to use Curtain MonGuard, which displays a layer of watermark on the screens of employees' desktop and laptop computers. The company can customize the watermark content and display settings, including font size, color, darkness, transparency, etc. The watermark content can include important information such as the current logged-in user, computer name, IP address, and date/time. If an employee captures confidential data using their mobile phone, the watermark content will be recorded along with it. If the data is leaked online, management can trace back to the individual responsible. This watermark serves as a reminder and deterrent, greatly reducing the chances of internal employees casually sharing data with others.

Additionally, the system allows for setting screen watermarks based on different users and specific conditions, such as specific time periods or being outside the company premises. The system also supports different usage scenarios, such as remote control and virtual desktop operations. Even during the COVID pandemic when employees need to use their home computers for remote control of company computers, the screen watermark will still be displayed, enhancing data security.

### Environment

Server-side:  
- Windows Server

Client-side:  
- Windows 10 & 11

### Products

- Curtain MonGuard



### **The Results**

- Effectively remind employees to handle the displayed content on the screen with caution when dealing with confidential data
- Reduce the chances of internal personnel casually sharing data with others
- Set screen watermarks based on different users and specific conditions to meet specific needs
- The installation, configuration, and future maintenance are all very simple

### **For more information, please contact us.**

Coworkshop Solutions Limited  
General Enquiry: (852) 2776 6161  
E-mail: [info@coworkshop.com](mailto:info@coworkshop.com)  
Website: [www.coworkshop.com](http://www.coworkshop.com)  
More case studies: [www.coworkshop.com/CaseStudies](http://www.coworkshop.com/CaseStudies)

