# Shutterfly reacts to data breach

By **Ian Murphy** - April 5, 2018

Web-based printing company Shutterfly has warned employees and former employees that their data may have been compromised. The breach was discovered on March 20 although the company is not saying how.

The company disclosed the breach in a filing with the Office of the Attorney General for California. It says that: *"On March 20, 2018, we learned that a Shutterfly employee's credentials were used without authorization to access our Workday test environment on January 11, 2018. We do not yet know if unauthorized access occurred at other times.*

*"This test environment is used by a limited number of employees to develop, test and preview Workday functionality before it goes live. As soon as we were made aware, our security team promptly implemented additional security measures. We do not believe that the security of the W*

## What data was a

The company says that th
includes: *"..name, social s*
*email; any passport num*
*bank account and routing*

*personal email that was on file in Workday; and the names, dates of birth, and social security numbers of any beneficiaries and/or dependents that were on file in Workday."*

Despite this treasure trove of data being accessed, Shutterfly claims that it has no evidence that any confidential information was taken. If it is right, then it has been very lucky. However, the notification raises a number of questions about data practices and potential reuse of employee credentials across multiple systems.

It is not unusual for organisations to use live data in test systems. The reason it is done is to ensure that testing is against real-world representative data. However, there are drawbacks to this. If you only test against what you know you don't detect system failure when people enter malformed data into fields.

The other question here is why was an employee not using separate credentials on the test data? The majority of successful credential breaches occur due to reused security credentials. Had the company required employees to use alternative credentials for the test system then the likelihood is that this breach would not have occurred. But that raises another, unanswered question. Were the credentials used elsewhere? At the moment, Shutterfly is implying no but until the investigation is completed, questions will remain.

## What is Shutterfl

Shutterfly is carrying out
working with an outside f
much more about what w
another statement. At tha

risk and what comes next.

For now, they are providing current and former employees with instructions on how to enrol with Experian's IdentityWorks. There is a free code that will be sent to them but they MUST sign up by June 30, 2018.

## What does this mean?

Another day, another breach. However, unlike most companies that seem to faff around and lose time, Shutterfly has made all the right moves. Details have been provided to the authorities, a forensic firm engaged and letters sent to those potentially affected. Some may question the delay between the breach and the discovery but the timescale here is still pretty short.

According to William Tsing, Malware Analyst, Malwarebytes:
*"Unauthorized use of employee credentials on a secondary network is often due to said employee reusing a work credential on a third-party site that gets breached. The other scenario is a simple phish masquerading as a corporate resource. Curbing the first behavior is almost impossible, so solutions generally include not using simple credential pairs for authentication to begin with.*

*"Companies with success against credential reuse tend to use a third identifier, or two-fa scenario comes from bet to a lesser extent, craftin they don't look like phish only to employees.*

*"The old answer to these else is no longer sufficien*

*include better systems design, as outlined in the examples above."*

**Ian Murphy**

*http://www.enterprisetimes.co.uk*

Ian has been a journalist, editor and analyst for over 35 years. While technology remains the core focus of Ian's writings he also covers science fiction, children toys, field hockey and progressive rock. As an analyst, Ian is the Cyber Security and Infrastructure Practice Leader for Synonym Advisory. A keen hockey goalkeeper, Ian coaches and plays for a number of clubs including Guildford Hockey Club, Alton Hockey Club, Royal Navy, Combined Services, UK Armed Forces and several touring sides. His ambition is to one day represent England. Ian has also been selected to be the goalkeeping coach for Hockey for Heroes, a UK charity supporting the UK Armed Forces.