What You Should Know About Data Breaches: Five Essential Steps to Reduce Losses

"An ounce of prevention is worth a pound of cure." Sure, we all know this, but there will be occasions when–despite everyone's best proactive efforts–trouble still arises. The ongoing war against cybercrime is no exception; setbacks are inevitable. Fortunately, there are ways to mitigate damages and see that fraudulent activity is not as lucrative as the scammers and thieves had hoped.

Following a data breach, the all-too common reaction might be a mad scramble of panicked activity that only wastes time while losses mount. By contrast, an effective response to such an event requires immediate and deliberate steps based on understanding the forces at work. Since the minutes following the discovery of a breach are hardly optimal for researching data security, it makes sense to have done a little reading on the subject ahead of time.

Data Breaches: A How, What, and Why

How do we define "data breach?"

Any confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion would be categorized as a data breach. The incident may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

Credit cards are still the most sold digital good on underground forums. Yet from 2009–2017, more than seven billion identity thefts have taken place through data breaches–approximately one for every person on the planet.

Source: Symantec Internet Security Threat Report, April 2017

PSCU

What You Should Know About Data Breaches: Five Essential Steps to Reduce Losses

What are we seeing with breaches?

Breaches are getting larger. Notably, breaches of payment card data at restaurants and fast food establishments are on the rise. However, the most alarming security failures have taken place at organizations that have complete identity profiles encompassing all of an individual's personal information identity.

The Equifax and Yahoo incursions are cases in point. These were game changers because it gave the fraudsters a complete identity profile on millions of Americans. The stolen data included addresses, dates of birth, social security numbers, genders, phone numbers, driver's license numbers (with issuing-state information), credit card numbers and tax IDs …frightening!

Why are breaches of personal information an important concern for credit unions?

It's easy to understand the risks of stolen payment information, but the Financial Risk posed by an identity-related breach can have a much broader impact on a credit union and its members. Criminals can use the credentials they obtained from a breach to generate an entire profile, thereby gaining access to members' existing card or their online banking. The fraudsters may even open up new accounts using the stolen information obtained from the breach. Therefore, authenticating account actions becomes increasingly important as fraudsters gain access to additional personal information which could be used to impersonate a legitimate member.

Of the 2017 data breaches (through June), 5.8 percent occurred in the banking, credit, and financial sectors, a jump from 3.6 percent in the first half of 2016.

Impact of Data Breaches

Data breaches have become so commonplace it's easy to forget that they have a real impact on people and the relationship they have with their financial institutions. The Identity Theft Resource Center's report, Identity Theft: The Aftermath 2016, found that nearly 20 percent of Americans surveyed were the victim of some kind of criminal identity theft in 2015. Of those, 9.2 percent said their identity was used to commit a financial crime that resulted in an arrest warrant. Nearly half of the respondents, 46 percent, reported fraudulent activity on existing accounts. Of those who experienced fraud on existing accounts, 22.4 percent said they changed credit card companies following the fraud.

There are also real dollars at stake. According to the 2017 Cost of Data Breach Study: United States, produced by IBM and the Ponemon Institute, the average cost of each lost or stolen record containing sensitive and confidential information is $225 per capita. Of particular interest to credit unions, the study also revealed that financial services ($336 per capita), had costs that are well above average. For that reason, it is more important than ever to be prepared for data breaches.

What You Should Know About Data Breaches: Five Essential Steps to Reduce Losses

Prepare Your Action Plan

The question now is what should a credit union do if there's been a breach of sensitive data involving members' cards or personal information? Here are the Five Steps to help you be prepared:

1. Ask your Processor about Dark Web Monitoring.

The dark web is often used by criminals to buy and sell stolen payment and personal information because it is not easily accessible through a traditional web browser such as Internet Explorer. This allows the fraudsters to operate their illicit businesses with a degree of anonymity from law enforcement. A dark web monitoring service scans the many online shops setup by fraudsters to find stolen payment information before it can be used by a fraudster to commit fraud on a member's account. This proactive approach can save your credit union much of the time and effort required to resolve and protect your members from a breach.

2. Enlist members in the battle.

On a regular basis (not just after a breach) utilize channels like your website, online banking, mobile app, statements and on-hold messages to encourage your members to monitor their accounts regularly. Promote solutions that help members be proactive in account monitoring. Encourage them to sign-up for transaction or account activity alerts (mobile apps are great for this!) so that they develop a habit for spotting suspicious activity. In a very visible place, always indicate what number to call or what to do if they feel there have been suspicious transactions involving their cards. Educating your members will help them to identify and report suspicious activity on their accounts in a more timely fashion.

3. Determine if re-issue is necessary.

There is no one-size-fits-all answer to the question of re-issuance, but it's a good idea to create a plan in advance to help determine when to reissue based on the severity of the compromise. Rely on reporting during a compromised event. Assess the number of accounts that have been breached. Evaluate the demographic information of the account holders to fully understand your exposure. Determine what percentage of the accounts affected by the breach are currently active. Identifying and striking a balance between the costs of reissue versus the gross/net fraud will be important to making the decision to re-issue. The chargeback process can be costly and sometimes it's prudent to just replace a card than to rely on the fact that you may be entitled to recovery. Reach out to your payments processor to utilize dedicated resources that will analyze this data for you and provide you with consultative recommendations for the best decision.

What You Should Know About Data Breaches: Five Essential Steps to Reduce Losses

4. Notify your members.

It's important to make sure your members are aware of the breach, the possible impact on them, and to share what your credit union is doing to mitigate damage and to keep the event from impacting their accounts. Utilize channels like email, online banking, mobile app and social media to make them aware of the breach. This will also let your members know what types of suspicious activity they might encounter due to the breach. Remember to be mindful of PCI-compliance regulations.

5. Educate your staff.

Your team has to know the plays! Make sure that key fraud-fighting -personnel at your credit union are continuously learning about current fraud trends and data compromises so they have their finger on the pulse of what is happening in the world. Document your breach process and ensure they are aware of the proper procedures so your plan will be carried out consistently when a breach arrives. Encourage your staff to leverage websites dedicated to fraud insights and subscribe to security-related e-newsletters. Consider sending a weekly fraud trends email to your employees to increase awareness of current breaches and fraud trends.

Remember, when it comes to protecting your members' most sensitive information and your credit union's assets (including your brand image), you can never be too prepared. And keep in mind that you aren't alone in this fight. PSCU has the expertise and resources available to assist you in every aspect of risk management and cybersecurity. Visit us at www.pscu.com or call 844.367.7728.

About PSCU:

PSCU, headquartered in St. Petersburg, Fla., is the nation's leading credit union service organization (CUSO). Founded in 1977 as a credit union cooperative, PSCU offers a comprehensive, highly integrated suite of payment solutions for credit unions to optimize their member experience. Today, PSCU supports the success of nearly 900 Owner credit unions representing 20.4 million accounts. Leveraging digital technology, PSCU provides secure, best-in-class solutions including payment processing, risk management, analytics, loyalty programs, marketing, strategic consulting and mobile platforms. Comprehensive, 24/7/365 member support is delivered by contact centers located throughout the United States. For more information, visit pscu.com.