BY JOHN HARRIS

Credit Union Data Protection Begins with the Right Identity Authentication Tools

It used to be that credit unions could ensure the identity of their members just by building personal relationships with them. But with online and cloud-based financial transactions becoming ubiquitous, such identification is suddenly trickier. Learn the tools you need to keep your CU's personally identifiable information safe from cyber criminals.

The higher we climb toward digital ubiquity, the more we expose our data to cyber vulnerability. In 2015 alone, there were 781 data breaches tracked – an 8.1 percent increase over 2014, according to the Identity Theft Resource Center. Credit unions spent an average of $226,000 in costs associated with merchant data breaches in 2014, per the National Association of Federal Credit Unions.

Financial information and personally identifiable information, both of which are commonly found among credit union digital documents and accounts, are extremely valuable to cyber criminals. That's why credit unions face more pressure than ever before to secure member data. The foundational element for this security begins with identity authentication measures.

Identity authentication, at its core, is the process of making certain that only the right people have access to sensitive information and documents. Many credit unions achieve this certainty simply by building personal relationships with their members – personnel know who the customers are when they walk through a door. Of course, asking for valid identification, like a driver's license, is common whether or not a personal rapport has been established. But when documents are signed with e-signatures or an account is accessed online from a member's home, credit union staffers lose that luxury. Identities are hidden behind a digital wall but they still need to be correctly verified.

Stacey Foster, vice president of member services with Bar-Cons Federal Credit Union in Columbus, Indiana, said her credit union uses identity authentication to ensure cloud-based transactions are secure and legitimate.

"Many of our members sign loan closing documents online by using secure e-signature technology," added Foster. "Because those loan documents are legally binding agreements, it is absolutely imperative that we have procedures in place to verify the right person has access to those documents and [that] they are, in fact, the right signers. Once those documents are signed, those parties owe us money, so authentication is as much of a bottom line issue as is it a cyber security issue."

With credit unions rapidly adopting cloud technology, which allows users to participate in digital transactions – even loan closings – anywhere at any time, there are many different identity authentication methods to consider. Each one may have a different outcome with regard to security and convenience.

Email-Only Authentication

Everyone has likely encountered email-only authentication before – even if it's just confirming you want to receive a weekly newsletter from a website. Email authentication prompts the user to click a link sent to his email account before he can proceed with e-signing any documents or retrieving information. The assumption is that only the user knows her email username and password, and since she clicked the link, she is indeed the correct party.

Email-only authentication is by far the most convenient identity authentication measure available, but it is also the least secure. Usernames and passwords can be easily compromised. And if one account is breached, it's likely not the only one. Seventy-three percent of online accountholders use the same password for multiple accounts, according to a TeleSign report. As such, email authentication is typically best suited for low-risk information and transactions.

Shared Secret Questions

Credit unions can also require members to provide their unique answers to selected personal questions – or "shared secret questions" – such as: "What was the street you grew up on?" or "Who was your best childhood friend?" Users are later asked for these answers when accessing information. It's added protection from email-only authentication, but like several other methods, it does require an extra step.

Text Message Authentication

Credit unions can also work with technology providers to send a one-time PIN code to a member's cell phone. The member first proves her identity via email and then supplies the code sent to her phone before she's granted access.

Text message authentication that follows email authentication is one of the most popular and user-friendly forms of two-factor authentication. This type of authentication combines something you know (your email username and password) with something you have (your mobile phone for receipt of the one-time PIN code) – since almost everyone today has a mobile phone.

Know Your Customer Authentication

Know Your Customer (KYC) authentication requires a user to divulge closely guarded information to prove his identity. This disclosure may include providing a date of birth or a Social Security number. The KYC method may also ask members to provide account numbers and passcodes to confirm their identity.

Because KYC requires authentication of sensitive information that is not easily known by others apart from the user, it can offer a higher level of security than email-only authentication.

Knowledge-Based Authentication

Knowledge-Based Authentication (KBA) is the most secure standalone form of identity authentication. Before accessing documents or information, the user is required to provide a date of birth and Social Security number that match public records. Once this matching is confirmed, she is then challenged with a series of multiple-choice questions that are based on 30 years of information found in public databases. These questions may ask about vehicle registrations, property ownership or any other personally identifiable details that exist in public records. If one of the questions is incorrectly answered, the member may be provided with two more questions that must be answered correctly.

While KBA is an excellent way to restrict unauthorized access to sensitive information, it requires several steps. And for some users, because the questions demand information that may stretch back many years, they can present obstacles, even for the correct user.

The Balancing Act

A credit union may decide to deploy several different types of authentication for different types of transactions and data. Ultimately, a CU must decide which tools provide an appropriate level of cyber defense without requiring unnecessary effort from the member. When only basic information is at stake, say if a member needs to e-sign a consent form, email-only authentication may be a desirable choice. But if a member has the ability to deposit, withdraw or transfer money within his account, those extra security steps are worth it – especially compared to what could happen if a fraudster breached the account.

For its loan e-signings, Bar-Cons Federal Credit Union chose to combine authentication elements. It deploys KYC but fortifies the process further by adding shared secret questions.

"Though Social Security numbers aren't widely known outside of the individual they belong to, they can be stolen," explained Foster. "So combining shared secret questions with KYC authentication that must match public records gives us and our members assurance that our loan transactions and information are kept secure, without putting much strain on the process. It was the right choice for us."

The right choice for one credit union may be the wrong choice for another – but the golden rule of authentication remains consistent: Any identity authentication used is substantially better than none at all.

John Harris is the chief technology officer at SIGNiX, a Chattanooga, Tenn.-based digital signature solutions provider that makes signing documents online safe, secure and legal for any business. SIGNiX offers the only independently verifiable, cloud-based digital signature solution, which combines workflow convenience with superior security. Learn more about what makes SIGNiX different at www.signix.com.