How safe is your data?

Four Questions to Ask About Data Security

HARLAND CLARKE® | PAYMENT SOLUTIONS

Amidst rising data security concerns, banks and credit unions are re-examining risks associated with check program providers.

"An epic year for data breaches" is how one data security industry publication described 2013, citing examples like the well-chronicled breaches at Target® and Adobe®.[1] The residual effect: Any industry handling sensitive consumer records took a fresh look at its practices. Likewise, regulators updated their rules about the security practices of third-party vendors.

As reported in the American Banker, the updated rules "require banks to step up their oversight of third-party vendors deemed crucial to their operations. Banks need to risk-score such vendors, conduct on-site visits, monitor them, and be extremely thorough in drafting contracts and service level agreements."[2]

Amidst rising data security concerns, banks and credit unions are re-examining the risks associated with their check program providers. "No doubt, there's a heightened awareness of fraud generally and a new sensitivity to unauthorized access of sensitive consumer data," said Joe Filer, Harland Clarke's VP and Chief Information Security Officer. "We hear about it from our clients."

Banks and credit unions can protect themselves by fully vetting check suppliers and explicitly enumerating vendor data security responsibilities. "Historically, that has been accomplished through a good security requirement and clear expectations in the contract language," Filer explained.

[1] American Banker, *Naked Security*, February 19, 2014

[2] American Banker Bank Technology News, *New Rules Force Banks to Decide Which Vendors are 'Critical,'* May 2, 2014

When evaluating check suppliers, financial institutions should consider a range of security issues and ask these key questions.

Banks and credit unions can protect themselves by fully vetting check suppliers and enumerating vendor data security responsibilities.

1. Does the supplier have an industry proven, comprehensive information security control framework?

An industry proven, comprehensive framework is an excellent indicator that the supplier has the controls in place to meet compliance requirements. A good security control framework can include activities like an in-house security program, physical security practices and policies, and Red Flag FACTA solutions. "We subscribe to ISO 27002, which is an established industry standard that outlines hundreds of potential control mechanisms," said Filer.

2. Does your supplier have ongoing maintenance and evaluation of the effectiveness of their security framework?

Having a framework is only one step in delivering an effective data security program. Ask your supplier if they also have ongoing activities to maintain the effectiveness of their program. "Continuous attention to the security framework is essential. It is one area where you might see differences in terms of a vendor's level of commitment," said Filer. Security testing, vulnerability analysis and annual disaster recovery testing demonstrate a continuing commitment to security framework cogency.

3. Does your supplier provide you with information and tools to help with verification and validation of the protection of sensitive consumer data?

With increasing regulatory attention on data security, financial institutions are expected to perform oversight of suppliers who handle sensitive consumer information. You should expect your supplier to provide you with documentation that demonstrates they are in compliance with the regulations related to the management of non-public information. Some actions that demonstrate compliance are completion of self-assessment surveys, annual privacy statements, Payment Card Industry (PCI) compliance and independent enterprise certification (e.g., Service Organization

Controls 1 and 2). "We understand how important it is to have visibility into the completeness of a data security program, so we provide our clients with a comprehensive package of compliance documents that makes validation much more effective and efficient," said Filer.

4. Does your supplier provide a structured oversight program for service provider relationships where sensitive consumer data is used?

Office of the Comptroller of the Currency guidance speaks to the fact that the financial institution's protection should extend throughout the supply chain. This has made it even more important that your suppliers have a structured oversight program with their own supply network. A supplier with a solid program will have a risk management program that classifies its vendors and monitors their data security programs. Annual control framework assessments, with periodic onsite visits, are hallmarks of a strong oversight program. The program should also include a documented summary risk assessment on any vendor that handles your account holders' sensitive data.

"If there's one change in the compliance landscape, it's that some financial institutions are now more 'checklist oriented,'" said Filer. The checklist approach, however, doesn't always reveal the greatest security value. What's most important when evaluating a check program supplier? "Find a vendor that can prove the efficacy of its controls and advocates for your institution," Filer advised.

If you would like to learn more about how Harland Clarke keeps your data secure, call **1.800.351.3843**, email us at **contactHC@harlandclarke.com** or visit **harlandclarke.com/DataSecurity**.