ConsumerDirect® Security Practice Summary

At ConsumerDirect®, security is central to our organization. You could say it's in our DNA. We go through rigorous procedures and hold ourselves to the highest standards to ensure all data is kept safe and protected.

Below are the practices that we perform routinely to establish compliance in our security.

PCI-DSS Compliant

ConsumerDirect® is Level 1 PCI-DSS compliant which means our networks, processes, and systems are audited annually by a certified third-party PCI-DSS assessment company. Although this compliance is specific to secure handling and processing of credit cards, we expand on it to cover the additional sensitive information we collect from our customers. As part of our compliance, our systems undergo rigorous monthly, quarterly, and yearly security scans.

Quarterly Security Scans

As part of PCI-DSS, our systems are thoroughly scanned quarterly for security vulnerabilities. The scans cover all our internal servers and public endpoints. If any security vulnerabilities are discovered, we act immediately to resolve the vulnerability.

TransUnion Strategic Partnership

As part of our strategic partnership with TransUnion, we are held to the same security standards as TransUnion. TransUnion has a complete set of requirements and guidelines for securely storing their customers' data and we are annually audited by TransUnion to ensure compliance.

Regular Website Security Scans

With every release of our software, we perform a full security scan. This is to ensure that we do not introduce any vulnerabilities that would allow a hacker to compromise our system.

AWS Strategic Partnership

We are proud to announce that our systems are 100% hosted by Amazon's AWS Cloud Service. As a strategic partner, Amazon covers many of the PCI-DSS requirements around physically securing our systems on their network.

For additional questions about our security practices, please contact Partner Support at partnersupport@consumerdirect.com.