CYBER INCIDENT RESPONSE PLAN (IRP)

Fintech Analytics LLC, doing business as CRED iQ (“CRED iQ”)

Note: This Plan was last updated on May 15, 2020

1. Purpose. The purpose of this cyber incident response plan ("IRP") is to provide a structured and systematic incident response process for all information security incidents (as defined in Section 4, Definitions) that affect any of CRED IQ's information technology ("IT") systems, network, or data, including CRED IQ's data held or IT services provided by third-party vendors or other service providers.

1.1. Specifically, CRED IQ intends for this IRP to:

(a) Define CRED IQ's cyber incident response process and provide step-by-step guidelines for establishing a timely, consistent, and repeatable incident response process.

(b) Assist CRED IQ and any applicable third parties in quickly and efficiently responding to and recovering from different levels of information security incidents.

(c) Mitigate or minimize the effects of any information security incident on CRED IQ, its customers/clients, employees, and others.

(d) Help CRED IQ consistently document the actions it takes in response to information security incidents.

(e) Reduce overall risk exposure for CRED IQ.

(f) Engage stakeholders and drive appropriate participation in resolving information security incidents while fostering continuous improvement in CRED IQ's information security program and incident response process.

1.2. CRED IQ developed and maintains this IRP as may be required by applicable laws and regulations.

2. Scope. This IRP applies to CRED IQ, its employees, contractors, officers, and directors; and CRED IQ's IT systems, network, data, and any computer systems or networks connected to CRED IQ's network.

2.1. Other Plans and Policies. CRED IQ may, from time to time, approve and make available more detailed or location or work group-specific plans, policies, procedures, standards, or processes to address specific information security issues or incident response procedures. Those additional plans, policies, procedures, standards, and processes are extensions to this IRP.

3. Accountability. CRED IQ has designated it’s Technology Consultant to implement and maintain this IRP (the "information security coordinator"). The information security coordinator shall be responsible for coordinating IRT activities, conducting post-incident reviews to gather feedback on information security incident response procedures and reviewing this IRP at least annually, or whenever there is a material change in CRED IQ's business practices that may reasonably affect its cyber incident response procedures.

4. **Definitions**. The terms defined below apply throughout this IRP:

4.1. "Personal Information" means individually identifiable information that CRED IQ owns, licenses, or maintains and that is from or about an individual including, but not limited to (a) first and last name; (b) home or other physical address, including street name and name of city or town; (c) email address or other online information, such as a user name and password; (d) telephone number; (e) government-issued identification or other number; (f) financial or payment card account number; (g) date of birth; (h) health information, and (i) any information that is combined with any of (a) through (h) above].

4.2. "Information Security Incident" means an actual or reasonably suspected (a) loss or theft of confidential or personal information; (b) unauthorized use, disclosure, acquisition of or access to, or other unauthorized processing of confidential or personal information that reasonably may compromise the privacy or confidentiality, integrity, or availability of confidential or personal information; or (c) unauthorized access to or use of, inability to access, loss or theft of, or malicious infection of CRED IQ's IT systems or third party systems that reasonably may compromise the privacy or confidentiality, integrity, or availability of confidential or personal information or CRED IQ's operating environment or services.

5. **Incident Response Team**. The incident response team ("IRT") is a predetermined group of CRED IQ employees and resources responsible for responding to information security incidents.

5.1. Authority. Through this IRP, CRED IQ authorizes the IRT to take reasonable and appropriate steps necessary to mitigate and resolve information security incidents, in accordance with the escalation and notification procedures defined in this IRP.

5.2. Responsibilities. The IRT is responsible for:

(a) Addressing information security incidents in a timely manner, according to this IRP.

(b) Managing internal and external communications regarding information security incidents.

(c) Reporting its findings to management and to applicable authorities, as appropriate.

(d) Reprioritizing other work responsibilities to permit a timely response to information security incidents on notification.

6. **Incident Response Procedures**. CRED IQ shall develop, maintain, and follow incident response procedures to respond to and document identified information security incidents. CRED IQ may, from time to time, approve and make available more specific procedures for certain types of information security incidents. Those additional procedures and checklists are extensions to this IRP.

6.1. Detection and Discovery. CRED IQ shall develop, implement, and maintain procedures to detect, discover, and assess potential information security incidents through automated means and individual reports.

(a) Automated Detection. CRED IQ shall develop, implement, and maintain automated detection means and other technical safeguards.

(b) Reports from Employees or Other Internal Sources. Employees, or others authorized to access CRED IQ's IT systems, network, or data, shall immediately report any actual or suspected

information security incident to the information security coordinator. Individuals should report any information security incident they discover or suspect immediately and must not engage in their own investigation or other activities unless authorized.

(c) Reports from External Sources. External sources who claim to have information regarding an actual or alleged information security incident should be directed to information security coordinator. Employees who receive emails or other communications from external sources regarding information security incidents that may affect CRED IQ or others, security vulnerabilities, or related issues shall immediately report those communications to information security coordinator and shall not interact with the source unless authorized.

6.2. Escalation. Following identification of an information security incident, the information security coordinator, or a designate, shall perform an initial risk-based assessment and determine the level of response required based on the incident's characteristics, including affected systems and data, and potential risks and impact to CRED IQ and its customers/clients, employees, or others. Based on the initial assessment, the information security coordinator, or a designate, shall take all action reasonably necessary and available to respond to the incident.

6.3. Investigation and Analysis. On activation, the IRT shall collaborate to investigate each identified information security incident, analyze its affects, and formulate an appropriate response plan to contain, remediate, and recover from the incident.

6.4. Containment, Remediation, and Recovery. Next, the IRT shall direct execution of the response plan it formulates according to its incident investigation and analysis to contain, remediate, and recover from each identified information security incident, using appropriate internal and external resources.

6.5. Evidence Preservation. The IRT shall direct appropriate internal or external resources to capture and preserve evidence related to each identified information security incident during investigation, analysis, and response activities. The IRT shall seek counsel's advice, as needed, to establish appropriate evidence handling and preservation procedures and reasonably identify and protect evidence for specific information security incidents.

6.6. Communications and Notifications. For each identified information security incident, the IRT shall determine and direct appropriate internal and external communications and any required notifications. Only the IRT may authorize information security incident-related communications or notifications. The IRT shall seek counsel's advice, as needed, to review communications and notifications targets, content, and protocols. The IRT shall report criminal activity or threats to applicable authorities, as CRED IQ deems appropriate. While the IRT may choose to authorize discretionary communications, certain laws, regulations, and contractual commitments may require CRED IQ to notify various parties of some information security incidents. If applicable to a specific information security incident, as required, the IRT shall:

(a) Notify applicable regulators, law enforcement, or other authorities.

(b) If an applicable breach of personal information occurs, prepare and distribute notifications to affected individuals.

(c) Notify CRED IQ's cyber insurance carrier according to the terms and conditions of its current policy, including filing a claim, if appropriate.

6.7. Post-Incident Review. At a time reasonably following each identified information security incident, the information security coordinator, or a designate, shall reconvene the IRT, others who participated in response to the incident, and affected work group representatives, as appropriate, as a post-incident review team to assess the incident and CRED IQ's response. The information security coordinator shall monitor and coordinate completion of any follow-up actions identified by the post-incident review team, including communicating its recommendations to and seeking necessary authorization or support from CRED IQ leadership.

Send any suggested changes or other feedback on this IRP to Support@cred-iq.com