Lodestone

SERVICE BRIEF FOR

PAYMENT FRAUD INVESTIGATION

Often coupled with other types of investigations Lodestone handles, including business email compromises (BECs) and insider threats, attempted and successful payment fraud is growing increasingly common.

Our experts are experienced in identifying key evidence and performing detailed analysis on the timelines around suspected payment fraud to help determine what happened and how. Receive findings and updates every step of the way, along with a final report that summarizes the work performed and the conclusions made.

BENEFITS

- Understand how a threat actor may have accessed your systems and performed or attempted to perform fraudulent activities.
- Receive a detailed report documenting the event, including root cause analysis, along with recommendations on hardening systems or policies to prevent fraudulent activity in the future.

OVERVIEW

Lodestone's Payment Fraud Investigation focuses on any threats and breaches to your payment platform or otherwise related to financial and banking information. Lodestone's investigations provide a detailed understanding of how a threat actor may have accessed your environment and the actions performed.

Lodestone analysts have deep experience handling countless cases of payment manipulations and redirections and stand ready to deliver knowledge, clarity, and solutions in the face of fraud or attempted fraud.

WHY LODESTONE

Lodestone is a global cybersecurity firm committed to helping clients prevent, investigate, and prepare for security incidents. It was built from the ground up to offer an innovative, behavior-based approach to proactive cybersecurity and digital forensics and incident response (DFIR). We are comprised of top investigative talent and offensive security experts from several of the world's largest cybersecurity firms, as well as military veterans and former members of national security organizations, including the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA). We combine this expertise with our unique understanding of legal requirements through our relationship with our parent company, Beazley, which has been at the forefront of cyber insurance for over a decade. Through this relationship, Lodestone has developed a unique understanding of the intersection between insurance and cybersecurity while preventing, preparing for, and responding to some of the toughest security challenges that industries face today.

Compliance

Since its founding as a subsidiary of Beazley in 2017, Lodestone has offered its customers insight into both cybersecurity and the cyber insurance industry. We help companies align and stay compliant with cyber insurance coverage requirements. In addition, we offer discounts to channel partners to form long-term relationships.

Security Focus

Lodestone's experts live and breathe cybersecurity and are committed to helping customers face some of the biggest challenges of their careers. We do not sell vendor security products – our offerings are purely service-focused, and any third-party tools we recommend are the product of genuine, vendor-agnostic, and tested endorsement, not business deals.

Expertise

Lodestone's approach to Incident Response is to have the top cybersecurity experts in the world, as the lead, and as the touchpoint, when responding to cybersecurity incidents. This is done with the backing of comprehensive, real-time threat intelligence to provide clients with protection across the life cycle of a potential security event or incident.

Tailored Approach

We understand the individual challenges of every situation and consider the human side of the equation, never taking a "one size fits all" approach. We blend design, threat intelligence, and technology with human insights to provide clients with the greatest cybersecurity advantage.

Threat Intelligence

Our deep understanding of threat actor tactics, techniques, and procedures (TTPs) is based on decades of experience in DFIR and the diligent gathering of threat intelligence from all possible sources.

Agility

Time is of the essence before, during, and after an intrusion. We stand ready to move in quickly and effectively at the first sign of an intrusion.

Team Experience

1000+
ENGAGEMENTS

200+ YEARS
COMBINED EXPERIENCE

50+
CERTIFICATIONS

Experts Unlike Anyone Else

EX-

MILITARY
LAW ENFORCEMENT
INTELLIGENCE
TOP CYBER TECH
TOP CONSULTING
FORTUNE 100 ENTERPRISE

Global Presence - NA/Europe

METHODOLOGY

A Payment Fraud Investigation is comprised of these primary phases:

Initial Response
Incident Containment and Mitigation
Evidence Collection
Investigation
Reporting
Conclusion and Recovery

- Initial Response – Lodestone works with you to determine the scope of the investigation, our initial impressions of any potential impact on the environment, and business objectives your organization may have.
- Incident Containment and Mitigation – Lodestone experts advise you on the fastest path to stopping the threat actors from performing more malicious activity and doing additional damage to your environment. We support you with the deployment of tooling and configurations with our expert insights and put controls in place to prevent further disruption during response and restoration.
- Evidence Collection – Our experts work with you to understand how a threat actor may have accessed systems and performed fraudulent activities and collect evidence accordingly. We use industry-standard tools and software and perform all necessary handling steps to address any legal considerations.
- Investigation – Lodestone analyzes the evidence collected to identify available indicators of compromise. We provide contextualization to the incident, including determining, if possible, the root cause, the malicious activity performed, and what unauthorized data may have been accessed or exfiltrated.
- Reporting – We provide a written final summary of the investigation with a concise description of the findings and details of the investigation for any historical preservation and reporting requirements you may have.
- Conclusion and Recovery – Lodestone answers your lingering questions and provides general industry best practices for cybersecurity to move your company forward. Throughout the engagement, we also work with your personnel to advise on a plan of action that can restore your network to not just its pre-incident state, but a safer one.

DURATION AND DELIVERABLES

Payment Fraud Investigations vary based on the size of the environment and the number of systems involved. However, this typically takes a period of one to two weeks.

As part of a Payment Fraud Investigation, Lodestone will provide any or all of the following upon request:

Executive Summary Report – A high-level summary report that provides an overview of the Payment Fraud Investigation, including key findings identified during the investigative process.

Digital Forensics and Incident Response (DFIR) Report – A detailed, technical breakdown of how the threat actor operated within your environment, including a granular list of affected systems and data, in addition to the information provided in an Executive Summary Report.

Executive Debrief – An overview of the investigation and key findings presented in-person or via video conference with our Case Lead.

Best Practices Overview – A generalized list of best practices that can help you strengthen your security posture against future attack.

Learn more at www.lodestone.com

Connect with us:

320 East Main Street, Lewisville, TX 75057, USA

Tel: +1-203-307-4984

info@lodestone.com

Lodestone Security is a wholly owned subsidiary of Beazley plc. Lodestone provides computer security and cyber security consulting services. Lodestone does not provide insurance services and client information obtained by Lodestone is not shared with Beazley claims or underwriting. Likewise, client information obtained by Beazley claims or underwriting is not shared with Lodestone.