SAMPLE — NOT LEGAL ADVICE. This response letter was generated automatically from publicly available analysis. It has NOT been reviewed by a licensed attorney and SHOULD NOT BE SENT to any party without substantial review and customization by qualified patent counsel. Use as a starting point only.

[Your Name]
[Your Title]
[Your Company]
[Street Address, City, State ZIP]

May 14, 2026

[Opposing Counsel Name]
[Firm Name]
[Address]

Re: U.S. Patent No. 7020281 — Response to Assertion of Infringement

Dear Counsel,

We acknowledge receipt of your correspondence asserting infringement of U.S. Patent No. 7020281 (the "7020281 Patent"). After preliminary review, we have substantial concerns about the validity, enforceability, and scope of the asserted claims, summarized below. We reserve all rights and defenses.

1. Subject Patent — Summary

A summary of US Patent 7,020,281, which is now expired, is provided below. A search of the United States Court of Appeals for the Federal Circuit (CAFC) 2026 dockets for this patent number did not yield any results.
Summary of US Patent 7,020,281
Title: Timing attack resistant cryptographic system
Assignee: The patent was originally assigned to Certicom Corp. and later assigned to Blackberry Limited. The current assignee is listed as Malikie Innovations Ltd.
Inventors:
• Ashok Vadekar
• Robert J. Lambert
Filing Date: January 18, 2001
Issue Date: March 28, 2006
Abstract:
The patent describes a method for performing a cryptographic group operation a specified number of times on an…

2. Validity Concerns under 35 U.S.C. § 102 — Prior Art

We have identified prior-art references that, in our preliminary view, anticipate one or more

asserted claims of the 7020281 Patent:

Prior Art Analysis for US Patent 7,020,281
This analysis details the most relevant prior art cited in US patent 7,020,281. The central innovation of the patent is a method to perform cryptographic operations in a way that is resistant to timing attacks, where an attacker analyzes the time taken for computations to deduce parts of the secret key. The patent's claims focus on two main approaches: ensuring each bit of a secret key is processed using similar, constant-time operations (Claim 1), and recoding the key into a signed-digit format to regularize the process (Claim 6).
The foundational concept of timing attacks was introduced in a 1996 paper by Paul C. Kocher, which is cited as a non-patent reference. Kocher's work identified the vulnerability in common cryptographic implementations, such as the square-and-multiply algorithm, where operations for a '1' bit take a different amount of time than for a '0' bit. This paper established the problem that US 7,020,281 and much of the cited prior art aim to solve.
Below are the most relevant patent citations and their potential impact…

3. Obviousness under 35 U.S.C. § 103

Independent of § 102, we believe the asserted claims are obvious in view of combinations of prior art that a person having ordinary skill in the art would have been motivated to combine:

Obviousness Analysis under 35 U.S.C. § 103
Under United States patent law, an invention is not patentable if "the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains." This analysis evaluates whether the independent claims of US patent 7,020,281 would have been obvious to a person of ordinary skill in the art (PHOSITA) at the time of the invention.
For the purpose of this analysis, a PHOSITA would be a computer scientist, mathematician, or electrical engineer with several years of experience in the field of applied cryptography. This individual would possess a strong understanding of public-key cryptosystems like RSA and Elliptic Curve Cryptography (ECC), the common algorithms used for their implementation (e.g., square-and-multiply, double-and-add), and the security vulnerabilities associated with physical implementations, specifically side-channel attacks like…

4. Litigation History of the Patent

Public records reflect that the 7020281 Patent has been the subject of the following litigation, which informs our view of the asserted claims and your client's enforcement posture:

• Malikie Innovations Limited v. Core Scientific, Inc. — U.S. District Court for the Eastern District of Texas · Ongoing

• Malikie Innovations Limited v. Marathon Digital Holdings, Inc. — U.S. District Court for the Western District of Texas · Ongoing

5. Request

In light of the foregoing, we request that your client (i) provide a detailed claim chart identifying each accused product or service and mapping every limitation of each asserted claim, (ii) identify any prior art known to your client, including any references cited during prosecution or reexamination, and (iii) substantiate the basis for any damages or licensing demand. We are prepared to discuss the matter further once we have received and reviewed the foregoing.

Sincerely,

[Your Name]