September 23, 2019

VIA EDGAR

Division of Corporation Finance
United States Securities and Exchange Commission
Washington, D.C. 20549

Re: Noodles & Company
Form 10-K for the Fiscal Year Ended January 1, 2019
Form 10-Q for the Fiscal Quarter Ended July 2, 2019
File No. 001-35987

To Whom It May Concern:

We are in receipt of the comments of the Staff (the "Staff") of the Division of Corporation Finance of the Securities and Exchange Commission (the "Commission") set forth in the Staff's letter dated September 13, 2019 (the "Letter") to Mr. Ken Kuick, Chief Financial Officer of Noodles & Company (the "Company"), regarding the Company's Annual Report on Form 10-K for the fiscal year ended January 1, 2019, filed on March 15, 2019, and the Company's Second Quarter Report on Form 10-Q for the fiscal quarter ended July 2, 2019, filed on August 6, 2019.

Each of your comments in the Letter is set forth below in italics, followed by our response. For ease of reference, the headings and numbered paragraphs below correspond to the headings and numbered comments in the Letter.

Form 10-K for the Fiscal Year Ended January 1, 2019

Risk Factors

We may be harmed by breaches of security of information technology systems..., page 12

1. *We note the disclosure here that you dedicate significant resources to preventing security breaches. We also note that you "have experienced many attempts to compromise [y]our information technology and data" and you "may experience more attempts in the future." In light of the data breach that occurred in 2016 and resulted in payments made through the year ended January 1, 2019, it appears that cybersecurity risks may be material to your business. Please revise your Risk Factors section to discuss that cybersecurity incident and its consequences as part of the broader discussion of the types of potential cybersecurity incidents that pose material risks to your business and operations. Your revised disclosure should consider this prior incident and its severity, the probability of the occurrence and potential magnitude of cybersecurity incident, the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, and the aspects of your business that give rise to material cybersecurity risks and the potential costs and consequences of such risks. See Item 503(c) of Regulation S-K and the Commission Statement and Guidance on Public Company Cybersecurity Disclosures dated February 26, 2018.*

Company's Response:

We acknowledge the Staff's comment. In response thereto, beginning with an expanded risk factor disclosure pursuant to Item 1A in our next Quarterly Report on Form 10-Q, we will include in our future filings revised disclosure in our

Risk Factors section that discusses the matters identified in the Staff's comment, substantially as indicated in the underlined language below.

We may be harmed by breaches of security of information technology systems or our confidential consumer, employee, financial, or other proprietary data.

We use many information technology systems throughout our operations, including systems that record and process customer sales, manage human resources and generate accounting and financial reports. For example, our restaurants use computerized management information systems, including point-of-sale computers that process customer credit card, debit card and gift card payments, and in-restaurant back office computer systems designed to assist in the management of our restaurants and provide labor and food cost management tools. Our franchisees use similar point of sale systems and are required to report business and operational data through an online reporting network. Through these systems, we have access to and store a variety of consumer, employee, financial and other types of information related to our business. We also rely on third-party vendors to provide information technology systems and to securely process and store related information. Our franchisees also use information technology systems and rely on third-party vendors. If our technology systems, or those of third party vendors we or our franchisees rely upon, are compromised as a result of a cyber-attack (including from circumvention of security systems, denial-of-service attacks, hacking, "phishing" attacks, computer viruses, ransomware, malware, or social engineering) or other external or internal methods, it could adversely affect our reputation, business, financial condition or results of operations.

The cyber risks we face range from cyber-attacks common to most industries to attacks that target us due to the confidential consumer information we obtain through our electronic processing of credit and debit card transactions. Like others in our industry, we have experienced many attempts to compromise our information technology and data, and we may experience more attempts in the future. For example, in 2016, we experienced a malware attack that compromised the security of the payment information of some customers who used debit or credit cards at certain locations between January 31, 2016 and June 2, 2016. We subsequently made payments of approximately $11 million to certain payment card companies for card issuer losses, card replacement costs and other charges issued by payment card companies, and incurred additional fees and costs associated with the data security incident, including legal fees, investigative fees, other professional fees, costs of communications with customers and capital investments for remediation activities.

Because cyber-attacks take many forms, change frequently, are becoming increasingly sophisticated, and may be difficult to detect for significant periods of time, we may not be able to respond adequately or timely to future cyber-attacks. If we or our franchisees, or third-party vendors, were to experience a material breach resulting in the unauthorized access, use, or destruction of our information technology systems or confidential consumer, employee, financial, or other proprietary data, it could negatively impact our reputation, reduce our ability to attract and retain customers and employees and disrupt the implementation and execution of our strategic goals. Moreover, such breaches could result in a violation of various privacy-related laws and subject us to investigations or private litigation, which, in turn, could expose us to civil or criminal liability, fines and penalties imposed by state and federal regulators, claims for purportedly fraudulent transactions arising out of the actual or alleged theft of credit or debit card information, compromised security and information systems, failure of our employees to comply with applicable laws, the unauthorized acquisition or use of such information by third parties, or other similar claims, and various costs associated with such matters.

We strive to mitigate the risk of breaches of our information technology systems and confidential data by enhancing our information technology networks and infrastructure, specifically in our physical and technological security measures, to anticipate cyber-attacks and defend against breaches, improving related procedures and controls and training our employees on cyber-security trends. While we have taken preventative measures to mitigate this risk, we can provide no assurance that we will not be the subject of cyber-attacks and data breaches in the future. Additionally, we carry cyber insurance to minimize the potential impact that a security breach may have on our financial condition or results of operations; however, liabilities incurred in connection with a security breach may exceed the limit that our data security liability insurer will pay or reimburse, in which case we would bear these fees and costs directly.

Although we dedicate significant resources to preventing security breaches, we may be unsuccessful, which could adversely affect our business, financial condition or results of operations.

Form 10-Q for the Fiscal Quarter Ended July 2, 2019

9. Leases, page 13

2. *We note your disclosure that some of your leases include rent escalations based on inflation indexes and fair market adjustments and that certain leases include contingent rental provisions that include a fixed base rent plus an additional percentage of the restaurant's sales. We also note that you recognize these subsequent escalations and contingent rental payments as variable lease expenses. Please revise the table at the top of page 14, which details the components of lease costs, to include the disclosure of variable lease expense, as well as short term lease expense. See ASC 842-20-50-4 for guidance.*

Company's Response:

We acknowledge the Staff's comment. In response thereto, we advise the Staff that variable lease expense year to date July 2, 2019 represents less than 0.5% of occupancy costs and is included within operating lease cost. Additionally, we have a de minimis amount of short-term lease expense and, therefore, have chosen to omit disclosure of such short-term lease expense on the basis that it is not material. We will include in our future filings, beginning with our next Quarterly Report on Form 10-Q, revised disclosure in footnote 9 substantially as indicated in the underlined language below.

Some of the Company's leases include rent escalations based on inflation indexes and fair market value adjustments. Certain leases contain contingent rental provisions that include a fixed base rent plus an additional percentage of the restaurant's sales in excess of stipulated amounts. Lease expense associated with rent escalation and contingent rental provisions is not material and is included within operating lease cost. Operating lease liabilities are calculated using the prevailing index or rate at lease commencement. Subsequent escalations in the index or rate and contingent rental payments are recognized as variable lease expenses. Our lease agreements do not contain any material residual value guarantees or material restrictive covenants.

3. *We note your disclosure that as most of the Company's leases do not provide an implicit rate, you used the incremental borrowing rate based on the information available at commencement date in determining the present value of lease payments. For those leases that do provide an implicit rate, please tell us if you use the implicit rate or incremental borrowing rate in calculating the present value of the lease payments.*

Company's Response:

We acknowledge the Staff's comment. In response thereto, we advise the Staff that for leases that do provide an implicit rate, which currently includes a de minimis number of leases, management determined that the use of the incremental borrowing rate was not materially different than using the implicit rate. After considering materiality, management utilized the incremental borrowing rate for these leases. The liability associated with leases that provide an implicit rate is approximately $1.0 million, which represents less than 0.5% of our $256.0 million lease liability. Management will continue to monitor the rates and will reassess the use of the implicit rate should the difference become material.

If you have any questions or require additional information concerning the above, please do not hesitate to contact me at (720) 214-1911.

Sincerely,

/s/ Ken Kuick

Ken Kuick
Chief Financial Officer

cc: Ms. Mel Heidman
Executive Vice President, General Counsel & Secretary, Noodles & Company

Mr. Andrew L. Fabens
Gibson, Dunn & Crutcher LLP

Mr. Jim Wilson
Ernst and Young LLP

The Audit Committee of the Board of Directors
Noodles & Company