Card Services

Card Risk Solutions

June 6, 2019

RO 19376

Fraud Trend – Quest Diagnostics Patient Data Compromise

☐ 311: Informational; No Action Required
☒ **611: Need to Know; Action May Be Required**
☐ 911: Urgent; Action May Be Required

Debit Card & ATM Programs
Credit Gateway Programs

Summary

This Trend Watch from our Risk Office discusses a compromise of Quest Diagnostics patient information and recommends actions to lower the risk of associated fraudulent activity, including identity theft and false authentication.

Quest Diagnostics recently disclosed that one of its third-party vendors experienced a data breach that exposed personal and financial information of nearly 12 million patients. Quest Diagnostics has publically stated that the compromise was discovered by American Medical Collection Agency (AMCA), a billing collections service provider used by one of its contractors, Optum360.

According to a statement on Quest Diagnostic's website:

> "AMCA first notified Quest and Optum360 on May 14, 2019 of potential unauthorized activity on AMCA's web payment page. On May 31, 2019, AMCA notified Quest and Optum360 that the data on AMCA's affected system included information regarding approximately 11.9 million Quest patients. AMCA believes this information includes personal information, including certain financial data, Social Security numbers, and medical information, but not laboratory test results.
>
> "AMCA has not yet provided Quest or Optum360 detailed or complete information about the AMCA data security incident, including which information of which individuals may have been affected. And Quest has not been able to verify the accuracy of the information received from AMCA.
>
> "Quest is taking this matter very seriously and is committed to the privacy and security of our patients' personal information. Since learning of the AMCA data security incident, we have suspended sending collection requests to AMCA. Quest will be working with Optum360 to ensure that Quest patients are appropriately notified consistent with the law."

Due to the suspected size and nature of the data stolen, this breach may be of interest to Fiserv clients.

In addition to the card information that may have been stolen, other data elements involved in this breach represent permanent markers of an individual's identity. A stolen identity, complete with birth date, Social Security number, and residence information, can be abused in ways that have greater and longer-term consequences than stolen card data. A stolen identity may be used to hijack existing bank accounts, obtain new credit or other services, conceal a criminal past, file fraudulent taxes, and even vote.

Risk Office recommends:

1. **Review** the processes you use to verify, identify and authenticate requests pertaining to new and existing accounts. If you are not using robust multi-factor authentication, this is the time to assess where token, out-of-wallet, geolocation, and/or device ID solutions could help detect fraud as it is attempted rather than after the fact. Fiserv offers the StepUp Authentication service, on both debit and credit platforms, to help increase security applied to incoming calls to our Fraud Center. If this service interests you, please contact your Fiserv - Card Services client executive for more details.

2. **Communicate** with your cardholders. Let them know why stronger authentication may be necessary given the recent increases in data breaches, and why they may now be asked for additional identity verification. Urge them to check all of their financial accounts on a regular and frequent basis. Encourage them to be skeptical about unsolicited email and telephone calls offering information or assistance related to the Quest Diagnostics breach.

3. **Share** information with your peers, regulators, business partners, and the law enforcement community regarding any attempted or successful fraud activities that may be related to recent breaches. We are all in this together.

Data breaches have become everyday news, but the reported incident at Quest Diagnostics may represent another challenging event for the financial services industry. Fiserv possesses no inside information on this data breach, nor do we have knowledge of any direct threat to our organization or your institution. This communication is offered based on our internal assessment of the incident's implications, in the spirit of helping our clients maintain the confidence of their customers and communities.

The Risk Office team will continue to monitor this event. We will provide updates should any new information become available.

If you have questions about risk strategies or need additional assistance, please contact us at risk_investigations@fiserv.com.