The Expert's View with Jeremy Kirk

Insights from industry experts

Finance & Banking , Fraud Management & Cybercrime , Fraud Risk Management

Home Loan Trading Platform Exposes Mortgage Documentation

Atlanta-Based MAXEX Left Software Development Platform Open

Jeremy Kirk (jeremy_kirk) • October 21, 2020

Loan trading platform MAXEX leaked documents submitted as part of mortgage applications, including this academic transcript.

There are few transactions that require more personal data than buying a home, which makes it imperative that all parties involved in each of the many steps in the process secure the data.

See Also: Threat Intelligence Solutions: A SANS Review of Anomali ThreatStream

But after a home is purchased, the risks to personal data aren't necessarily over. A data exposure by MAXEX, an Atlanta-based residential mortgage trading company, underscores the opaque transfer of personal data and the risks that come with it - even years later.

> "This has been a very stressful time, and we have spent hours contacting the credit agencies, closing accounts and changing passwords. I really hope no one else has to go through this nightmare."

MAXEX exposed 9GB of its internal data, much of which deals with software development for its loan-trading platform. But the data also included confidential banking documents, system login credentials, emails, the company's data breach incident response policy and even reports from penetration tests done several years ago. Plus, the company leaked complete mortgage documentation for at least 23 individuals in New Jersey and Pennsylvania.

The mortgage documents range from 400 to 600 pages for each individual. The PDFs contain an astounding amount of personal and financial data for those affected. The 23 documents relate to mortgages taken out around 2013, with personal documents included for several years prior to the mortgage application filing.

An example of a Form W-2 leaked in the mortgage documents

The documents include full tax returns; IRS transcripts; credit reports from the major agencies; bank account statements; scans of birth certificates, passports and driver's licenses; letters from employers, divorce records, academic transcripts and even Social Security numbers for not only the mortgage applicants but also their children.

In a statement on Wednesday, MAXEX said it it has retained leading security experts, contacted law enforcement agencies. After I notified the company of the breach on Oct. 7, it hired Mandiant, FireEye's computer forensics unit that traces the source of a breach and provides remediation advice. It has fixed the issues that lead to the breach.

"Based on the investigation thus far, it appears that the data from the systems accessed is limited to internal business information and a small number of loan files," MAXEX says. "We are in the process of contacting those affected."

MAXEX says its mortgage trading platform was unaffected. "The data was not in our exchange environment, and there is no indication that our exchange was compromised in any way."

Links to the data are now circulating on forums where stolen data is posted. On one platform, the data has been downloaded more than 1,000 times.

That's concerning to those affected, including a manager at a packaging manufacturer on the East Coast, who did not want to be identified by name for fear someone could look for his data. He's never heard of MAXEX and was alarmed when I contacted him. He's been the victim of identity theft schemes before.

"To be honest, I'm really concerned about my children," he says, noting that his kids' Social Security numbers and birth dates were exposed. "They're not even teenagers yet."

What Is MAXEX?

MAXEX has developed a digital exchange for buying and selling residential home loans, which is called the "secondary" mortgage market. Local banks extend home mortgages to consumers, but those loans are sold to entities such as Freddie Mac, Fannie Mae or other institutions, which bundle them up into securities.

Consumers consent to have their personal data transferred to other companies in this complex chain. Consumers don't have a choice in this if they want a mortgage. But this trading has immense benefits for homeowners, including long-term fixed interest rates.

MAXEX entered the market around 2013 with venture capital funding. Its intention is to disrupt the secondary mortgage trading market by using technology to overcome inefficiencies in how the market operates. Its platform lets banks sell their mortgages to a wider group of institutional investors, the company says.

As part of that process, MAXEX conducts due diligence on the loans that it offers on its marketplace to ensure a loan offered for purchase meets an investor's underwriting standards.

How the Leak Happened

The leaked MAXEX data started circulating around Sept. 29. A link to it was posted in a Telegram channel run by Tillie Kottmann, a Switzerland-based Android developer who hunts for data exposures.

Kottmann often releases data he finds on Telegram as well as in a GitLab group called Confidential & Proprietary. I've written about Kottmann before, and he was recently involved in distributing 20GB of corporate information that came from Intel (see: *Intel Investigating Possible Leak of Internal Data*).

Since he posted the MAXEX data, the link to it has popped up in other forums for sharing stolen data. Alex Holden, CISO for Hold Security, a Milwaukee-based security consultancy, found the data in a long-running Russian-language forum and passed it along to me.

I pinged Kottmann on Telegram to ask him some questions. He told me that he used the Shodan search engine to discover that MAXEX had a publicly exposed Jenkins server. Jenkins is widely used software for testing and developing other software applications. The open Jenkins server contained authentication credentials for two other development and collaboration platforms, Atlassian's Jira and Confluence.

"They [MAXEX] have a publicly exposed Jenkins server where the build logs of a [software] test that uploads results to Jira had Jira credentials in plain text," Kottmann says. "That account had enough permissions to have access to most spaces on both Jira and Confluence and also access to the backup feature in those products."

Holden says that statement shows that, not only could someone such as Kottmann have downloaded the data, but bad actors could have controlled Jira and Confluence, which could have led to other types of cyberattacks.

Alex Holden

"Within systems like Jira and Confluence, I can imagine that a malicious actor could spy on the data flows, steal sensitive data, get certain confidential data," Holden says. "But pivoting from access like this, a malicious actor can influence the product by spying on impending changes, including open security vulnerabilities. Also, in repositories like this, if login credentials are exposed, then the actor might actually change the product, data flows, data, etc."

I asked Kottmann why he posted the MAXEX sensitive personal data online. Even though the mortgage documentation dates to around 2013, much of it is static data that doesn't change, which puts those exposed at risk of identity theft.

Kottmann tells me: "I did kind of check for financial data, and all I personally found was sample data. Because that's [sensitive mortgage data] generally something I wouldn't want to release."

Kottmann has since removed a link to the MAXEX data from his GitLab group. But the data has propagated to other forums, meaning it likely will never be completely removed from the internet.

Breach Notification

I attempted to reach other people who had their mortgage data exposed, but I had no luck. That's not surprising, as people are likely justifiably wary of a journalist in Australia contacting them out of the blue saying he has all of their mortgage data.

The leak victim who's a manager at a packaging manufacturer tells me he filed a police report about the incident in order to get credit bureaus to lock his credit record for seven years. He says the police detective suggested that the file I sent him containing his mortgage data may have infected his computer with malware.

A copy of a birth certificate that was included in the exposed mortgage data

MAXEX says it is contacting those affected. Georgia, where MAXEX is based, has a mandatory breach notification law.

I put the manager at the packaging manufacturer in touch with MAXEX, which first offered him two years' worth of free credit monitoring. He says he requested longer coverage for his wife and children. MAXEX, he says, upped it to five years for his entire family.

But he worries that the leak puts him and his family at risk of identity theft for much longer than that.

"This has been a very stressful time, and we have spent hours contacting the credit agencies, closing accounts and changing passwords," he says. "I really hope no one else has to go through this nightmare."

About the Author

Jeremy Kirk

Managing Editor, Security and Technology, ISMG

Kirk is a veteran journalist who has reported from more than a dozen countries. Based in Sydney, he is Managing Editor for Security and Technology for Information Security Media Group. Prior to ISMG, he worked from London and Sydney covering computer security and privacy for International Data Group. Further back, he covered military affairs from Seoul, South Korea, and general assignment news for his hometown paper in Illinois.