Corporate **Identity Study**

Analysis and findings prepared
for **Company X**

InfoArmor

Methodology

Credit-related data

InfoArmor obtained the information for this report from a census file delivered by Company X. With Company X's permission, InfoArmor brought this census file to TransUnion for their data. TransUnion sourced the necessary attributes and delivered to InfoArmor anonymized data that we analyzed. That analysis provides the insights for this study.

TransUnion was able to correlate the data to 4,631 Company X employees. Credit-specific information, such as credit scores and number of inquiries, came only from TransUnion and was not shared with other credit bureaus.

Advanced threat intelligence data

InfoArmor's dark web intelligence team ran a database scan of all the domains of Company X and their subsidiaries. We looked for compromised IP addresses, domains, and credentials to determine if any emails, passwords, or websites were compromised or found in data sets, botnet logs, or known infected hosts. All the information we used, such as domains and social media accounts, is publicly accessible information that our intelligence team found.

Top findings

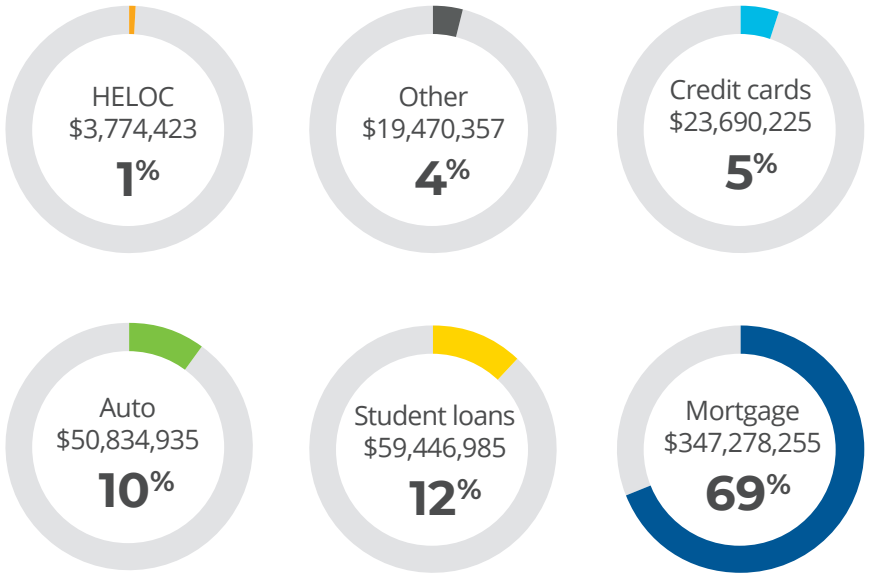
Based on the analyzed data, here are the most notable findings:

- Employees as a group still owe 78 percent of their account debts. And since only 7 percent of Company X employees have no debt, this means that most of the 93 percent who do have debt still have a majority of their debts left to repay.
- Company X employees have lower credit scores than the national averages. They have 6 percent fewer employees with Good or Excellent scores, and 9 percent more employees with Very Poor or Poor scores.
- A sizeable minority of employees are delinquent on payments. Thirty-seven percent have at least one account in collections. The most common burdens are student loans, auto loans, and credit cards.
- For those employees with student loans on their credit profile, 900 have been 90 days or more delinquent in at least one point since the debt was established.
- Younger employees are the most likely to have student loans. Forty percent of Millennial employees have at least one student loan, followed by 31 percent of Generation Z employees.
- Across generations, the average balance for an employee with at least one student loan is $39,268.
- Older employees are more likely to have a mortgage: More than double the number of Baby Boomers (46 percent) have mortgages than employees in Generation Z (22.8 percent).
- Company X employees are not close to paying off their mortgages. Of the 1,613 employees with at least one a mortgage, 97 percent still owe more than 50 percent of their mortgage. The average remaining balance on a mortgage is $195,559.
- Generation X and Millennials comprise 80 percent of Company X's workforce. Gen Xers have higher credit scores than Millennials, but carry more debt overall, mostly due to mortgages.
- Company X employees are using their work emails for non-work uses, and those accounts have been exposed in 16 separate breaches. This puts Company Xs brand reputation at risk and opens employees up to social engineering if data is exposed on a non-affiliated website.
- Company X botnet activity:
  - Botnet source 1 — We found a Company X-affiliated username associated with a botnet, exposing usernames and passwords for any sites that users visited.
  - Botnet source 2 — We found two infected computers associated with Company X and Company X email addresses. One infected computer may be an administrator account.

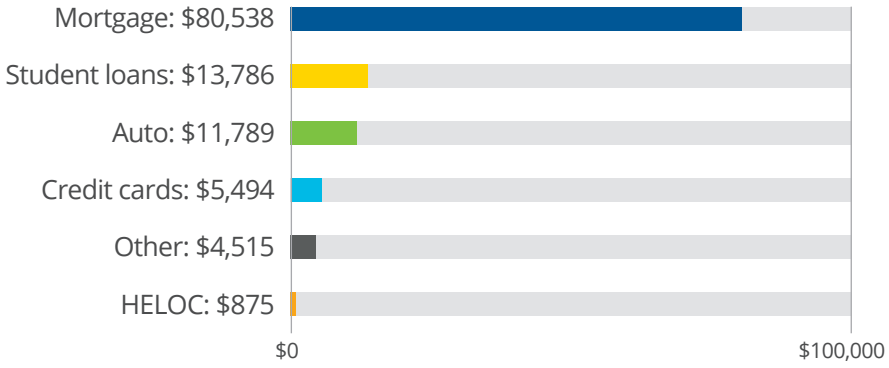
See **Recommendations** at the end of this study for further details

Your employee profile

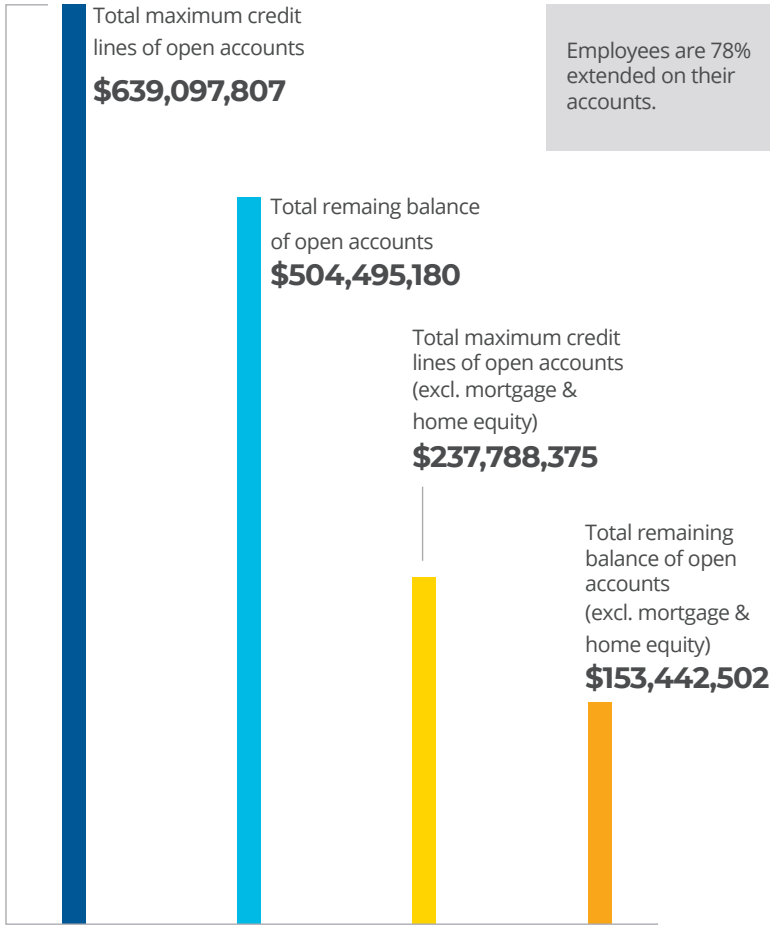
Total debt by source: **$504,495,180**



Average employee debt by source:

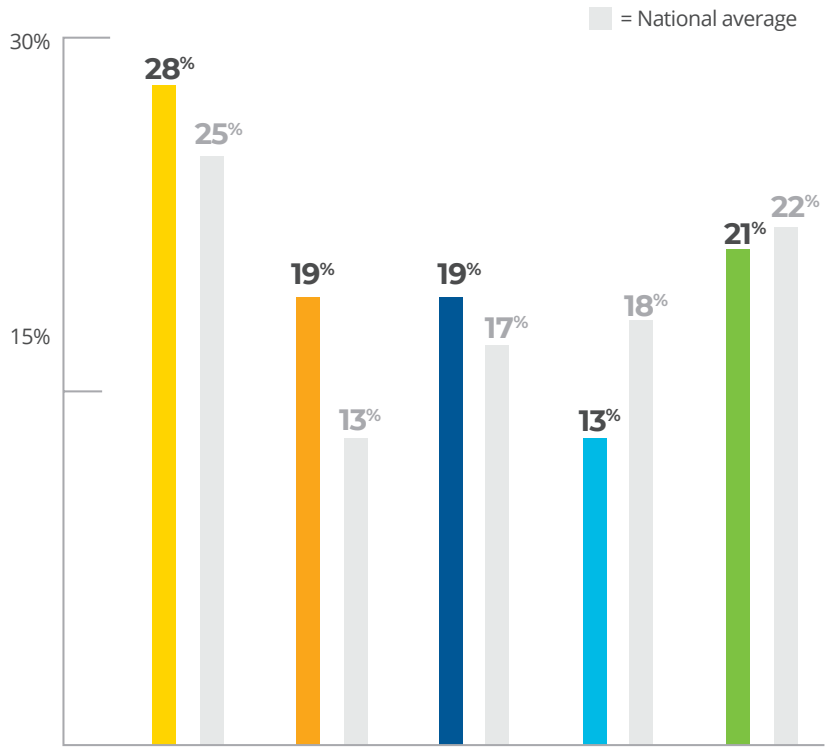


Account balances & credit lines:

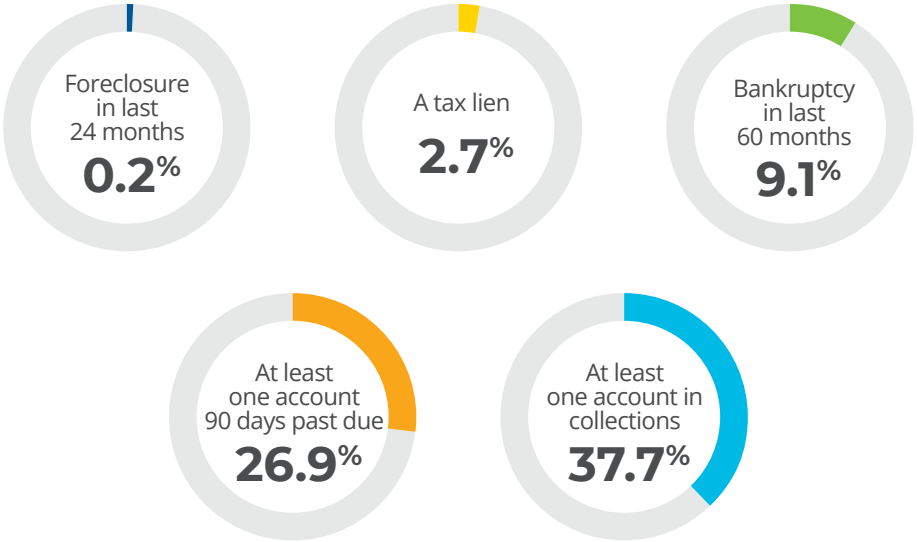


Employee credit worthiness

Employees scores vs. **national averages:**



Percent of employees with **negative credit items:**



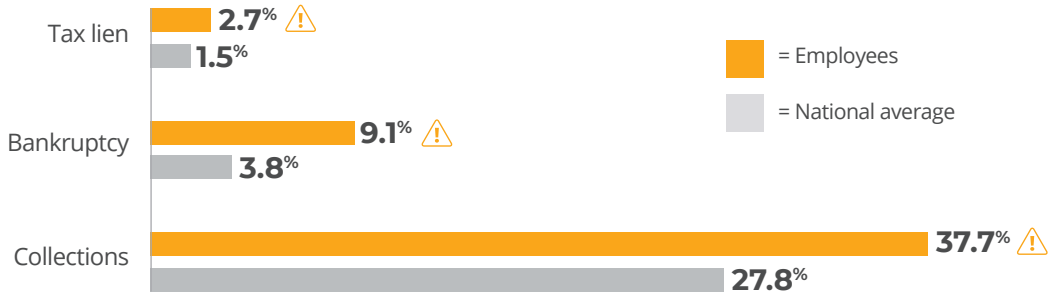
Satisfactory open accounts:
29,586

Delinquent open accounts:
2,375

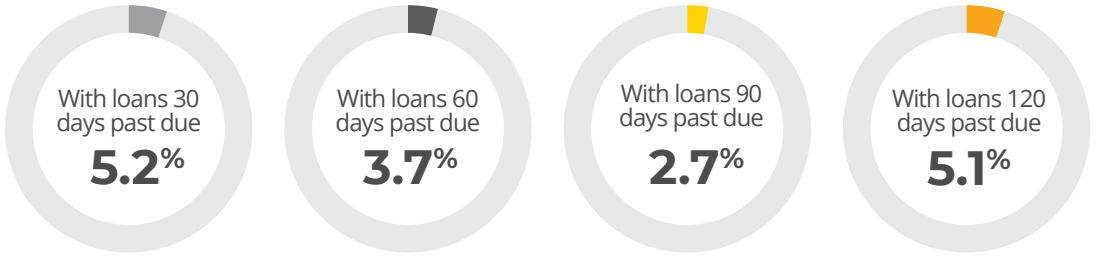
Employees with no debt:
7%

Financial stressors

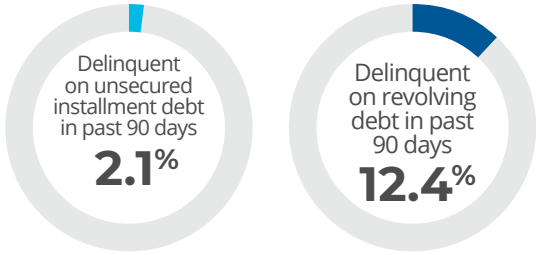
Significant employee **stressors:**



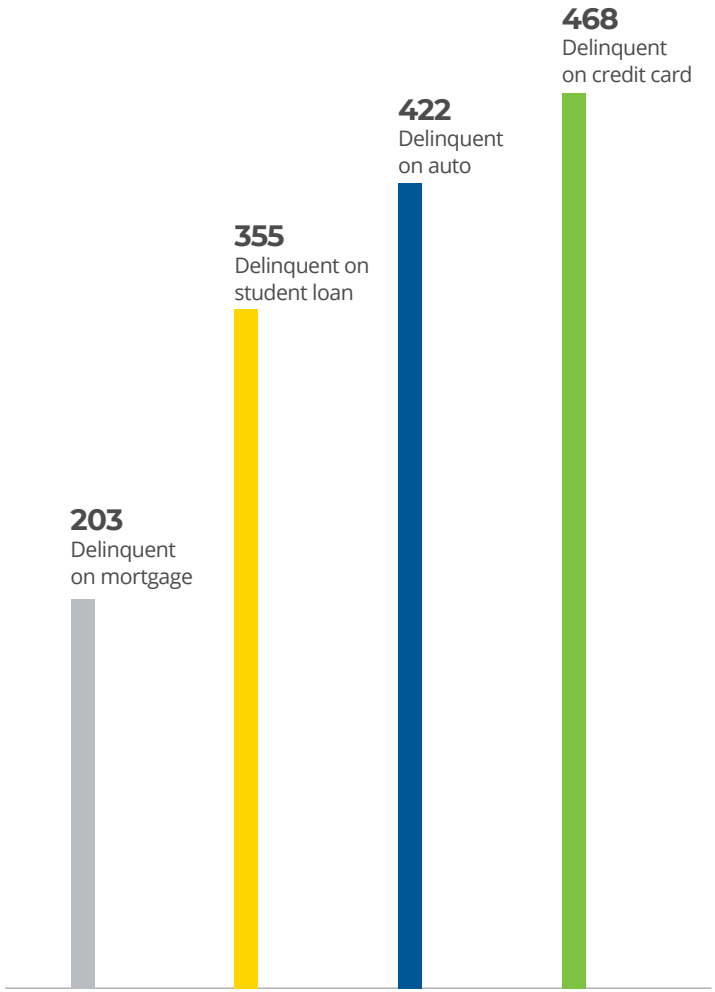
Employees with **loans past due:**



Employees with **delinquencies:**

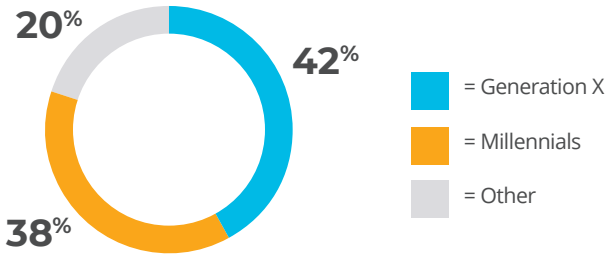


Employee financial burdens in past 90 days:

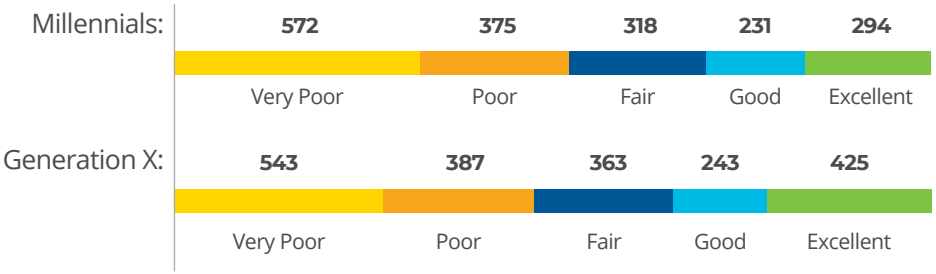


Generational breakdown

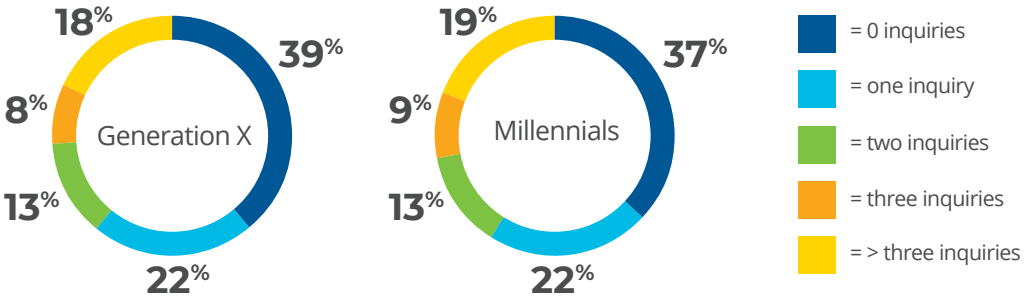
Employee **generational groups:**



Credit distribution by **age generation:**

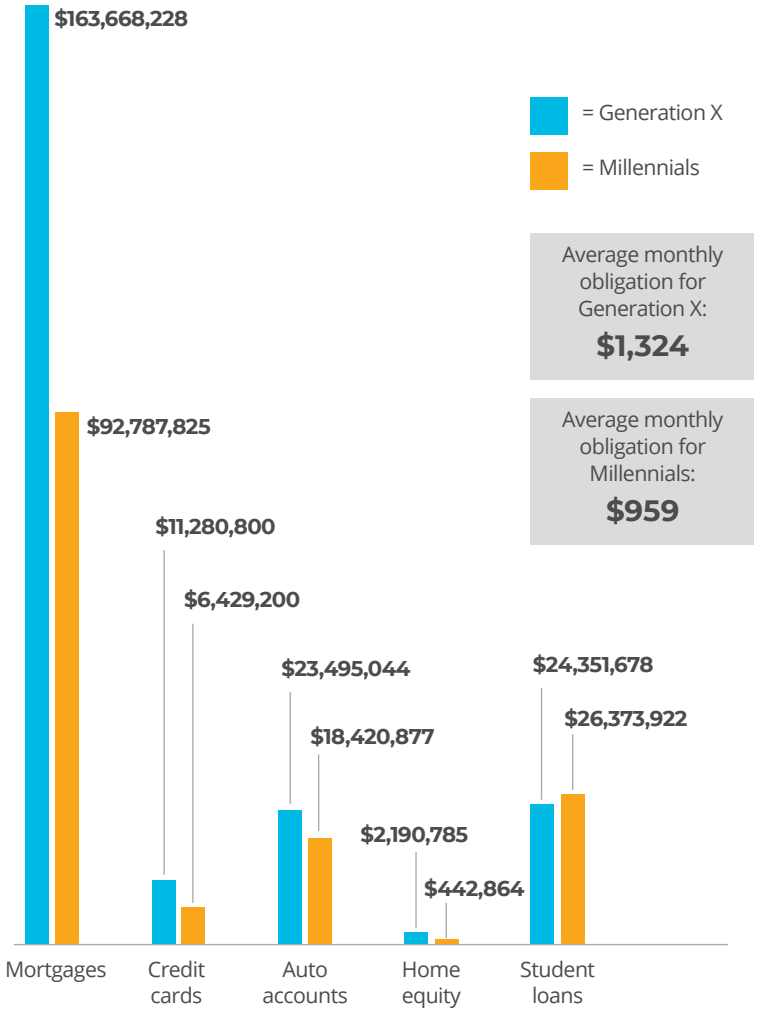


Number of **credit inquiries in past 12 months:**



Total balances by category:

(Verified in past 12 months)

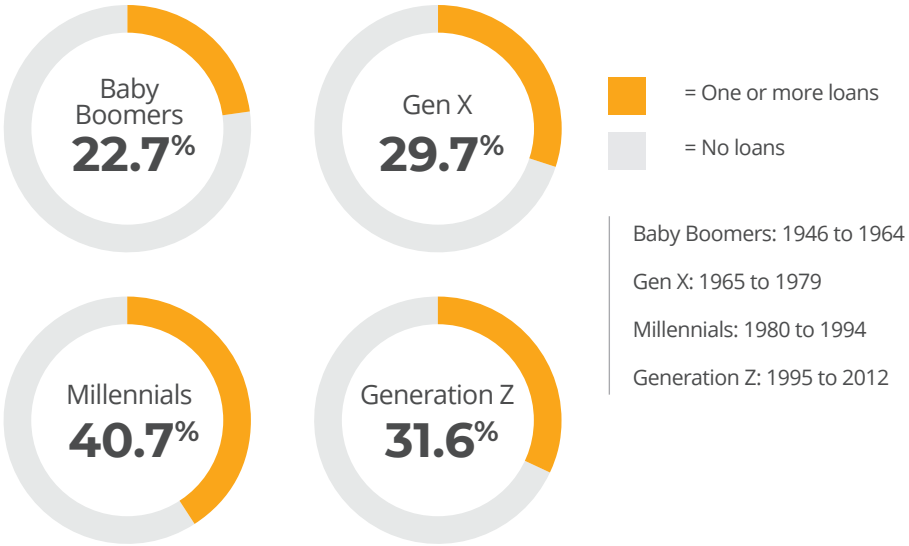


Average monthly obligation for Generation X:
$1,324

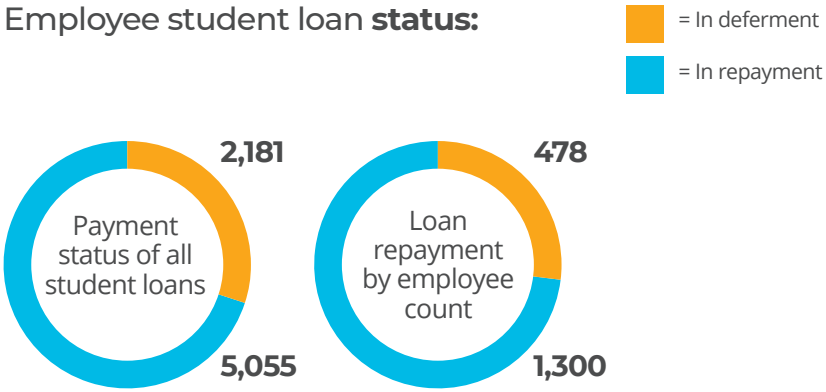
Average monthly obligation for Millennials:
$959

Student loan breakdown

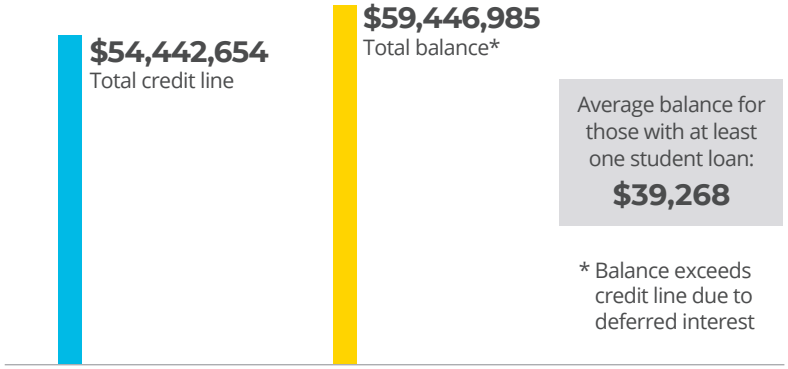
Student loans by **generation:**



Employee student loan **status:**



Student loan **balance** vs. **credit line:**



Employees with:

One student loan
11.6%

Two student loans
6.3%

> Two student loans
14.8%

Employees with student loan **delinquency in:**

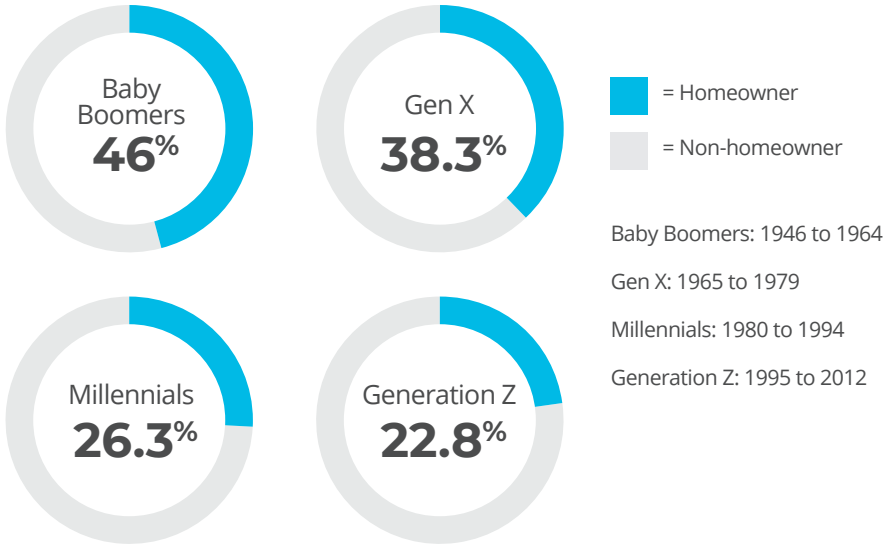
Past 90 days:
355

Past 180 days:
408

Past 365 days:
494

Mortgage breakdown

Home ownership by **generation:**



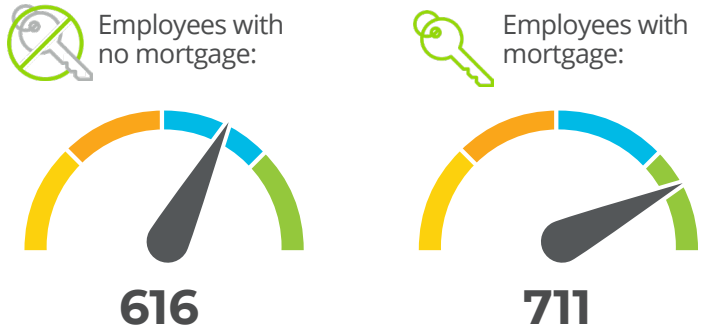
Baby Boomers: 1946 to 1964

Gen X: 1965 to 1979

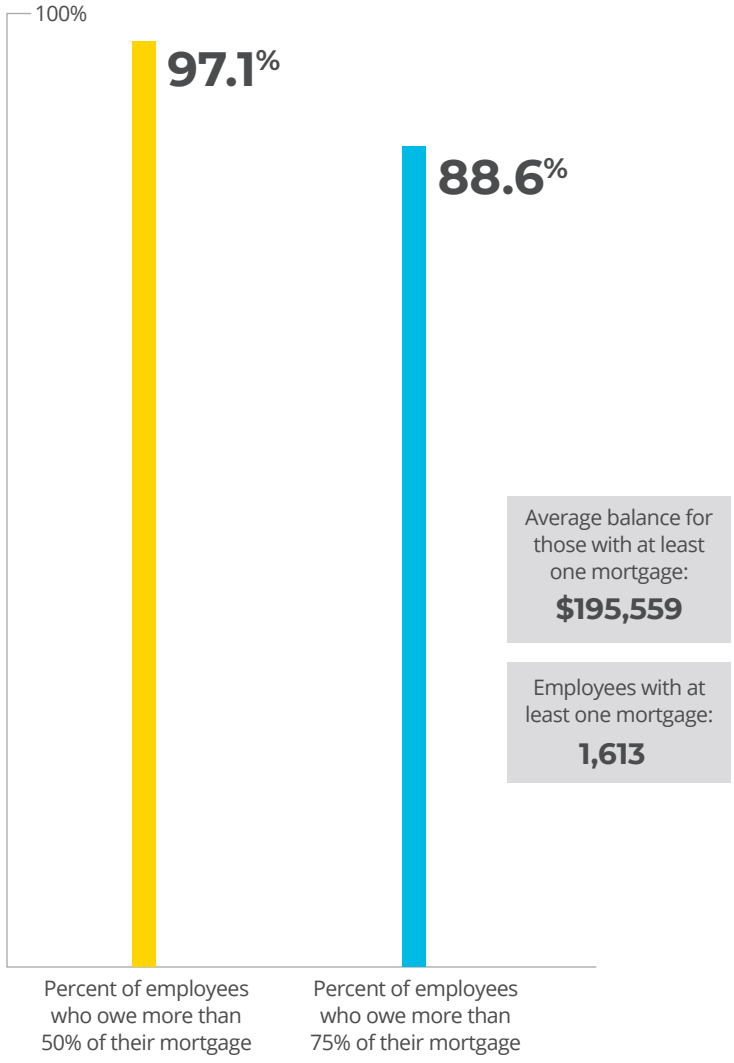
Millennials: 1980 to 1994

Generation Z: 1995 to 2012

Average **credit scores** of:



Balance vs. credit line:



Average balance for those with at least one mortgage:
$195,559

Employees with at least one mortgage:
1,613

Credentials found in data breach

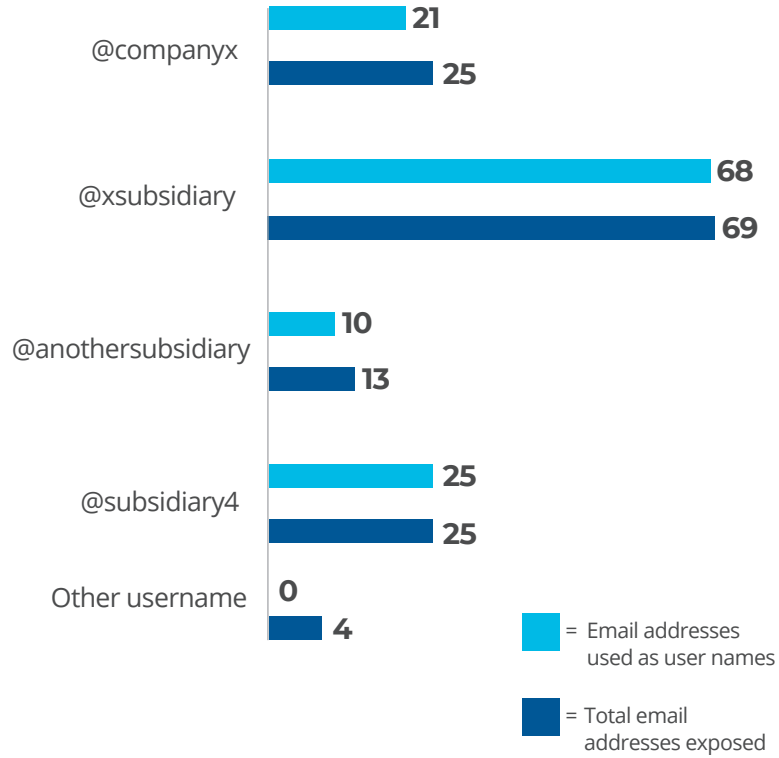
Username, email, and password exposure:

Total number of breaches with Company X data:

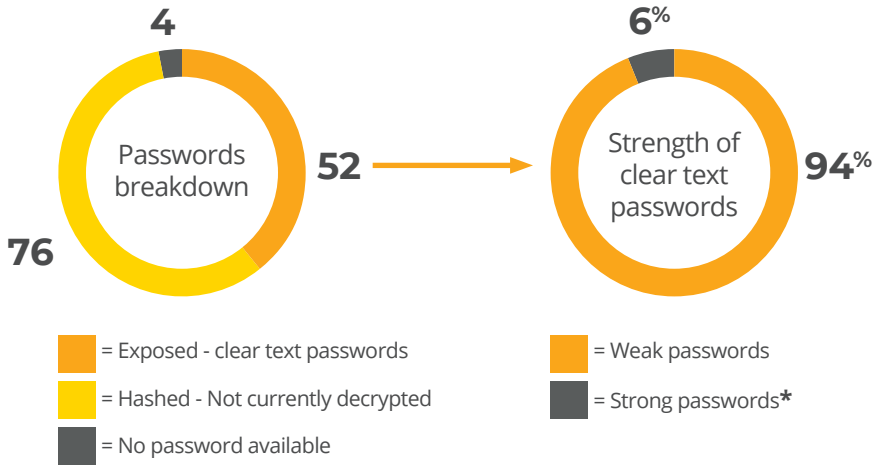
16

Total exposed credentials:

132



Total exposed passwords:



*A strong password consists of at least six characters that are a combination of upper and lowercase letters, numbers and symbols (@, #, $, %, etc.).

Examples of bad passwords:

Contains a Company X company or subsidiary name:

4

12345h:

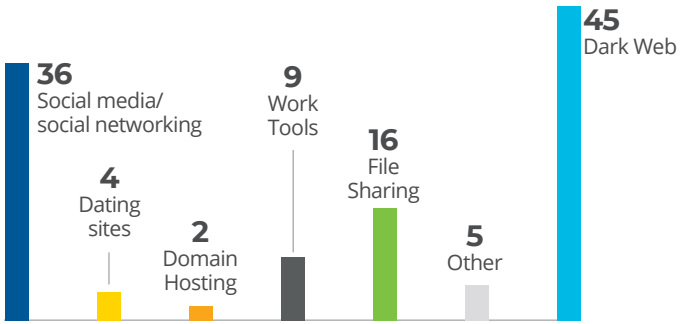
1

Email prefix as a password:

1

Breach sources and botnets

Data breach source breakdown:



Client credentials by breach source:

Company	Total	Category
Ashley Madison	1	Dating site
Webhost	1	Domain hosting
Adobe	9	Work tools
Badoo	1	Dating site
Dropbox	16	File sharing
Edmodo	1	Education site
Forbes	2	Media company
Altra Literature	1	Industrial manufacturing
Hostinger	1	Domain hosting
IBSG	1	Gaming
Mate1	2	Dating site
LinkedIn	33	Social media
Tumblr	1	Social media
Twitter	2	Social media
Dark Web	45	Dark Web

Botnet data:

A botnet is a network of private computers infected with malicious software and controlled as a group without the owners' knowledge.

We found through our sources that specific usernames were associated with a botnet that was either an email address associated with you or an infected user logged in to one of your websites.

The username and passwords to these sites have been compromised.

Machines infected: **2**

Users exposed: **2**

@companyx email address used as username: **4**

Site logins recorded by Botnet Source 1:

Site logins	Username
http://portal.companyx.com/Account/Login.aspx	100227351
http://infectedsite/learning.com/login	jdoe@companyx.com
https://procurementordering/companyx/Login	jdoe@companyx.com
https://www.companyxompanystore.com/	jdoe@companyx.com
	jdoe@companyx.com

See **Recommendations** at the end of this study for further details

Recommendations

Given InfoArmor's findings, here are the top recommendations we have for Company X:

- Employee benefits like student loan repayment assistance or tuition reimbursement would likely provide high value to Company X's employee population, especially in the younger generations.
- 401(k)/403(b) matching would provide substantial value, as many employees are still working to pay off significant amounts of debt and may not be able to save enough for retirement.
- An employee assistance program that includes financial counseling may be valuable to Company X employees.
- A life insurance plan may be beneficial for employees with debts who worry about providing for their families in the event of their untimely passing.
- Offering PrivacyArmor to all employees will provide knowledge regarding credit activity and alleviate the burden of identity theft remediation. Offering PrivacyArmor as an employer-paid option provides extra value in helping employees fully protect their future.
- Promoting security training will help eliminate the risk of employees using unsecure passwords and usernames across multiple accounts.
- Restrict employees from using their Company X credentials for non-corporate accounts.
- The results found during our botnet investigation should be addressed immediately.
  - **Botnet source 1—** The URLs and usernames found below were associated with either a Company X affiliated website or a Company X email address. We suspect that a computer used to log in to these sites was infected with a botnet. We recommend changing the passwords for these users on Company X impacted websites, and notifying the users to change their passwords for any other accounts they have used. We were unable to locate an IP address for these users so there we are not able to provide the name of the device that was infected.
  - **Botnet source 2 —** We found two computers associated with Company X that have been infected with a botnet. Computer 1 is named Anonymous with an IP address sourced in North Andover, MA. Computer 2 is named Admin-PC with an IP address sourced in Brampton, Ontario. The two infected computers should be located, their status determined, and appropriate action taken, which may include wiping the computers. The URLs visited and logged are:
  - https://outlook.office.com/owa/service.svc?action=adakjd;alfjkad;lfjad
  - https://outlook.office.com/owa/service.svc?action=adlkajfd;ldjkadlkjf
  - https://apis.google.com/u/0/_/adflkajdf;alkdjfa;ldkjfa;ldkjfad;lskfjad
  - https://pcompanyx/lookup/companyxpeople
  - At a minimum, credentials used on the machines that visited these sites should be changed immediately.