IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

KAS SCHAFER, an individual,
on his own behalf and on behalf of all
others similarly situated, and INTEGRITY
FIRST BANK, on its own behalf and on
behalf of all others similarly situated,

Plaintiffs, Civil Action #

v.

TARGET CORPORATION,
and TARGET.COM,

Defendants.

CLASS ACTION COMPLAINT

INTRODUCTION

1. Target is a Minnesota corporation headquartered in Minneapolis, Minnesota. Defendants represent the second-largest discount retailer in the United States and as of 2013, is ranked 36th on the Fortune 500 list of top US Companies, by revenue. Between at least November 27, 2013 and December 15, 2013, cybercriminals accessed insufficiently protected computer systems belonging to Target. As a result of Defendants' failure to properly secure their systems, the hackers obtained extensive personal information belonging to what is now estimated to be as many as 110 million Target customers, including but not limited to names, phone numbers, home addresses, credit and debit card numbers, PIN numbers, expiration dates, magnetic strip information, and passwords (hereinafter "personal identifying information").

2. Defendants Target Corporation and Target.com (collectively "Target," or "Company,"), failed to safeguard the confidential personal identifying information of consumers who made purchases at Target stores located in Wisconsin, and Wisconsin residents who made on-line purchases, between at least November 27, 2013 and December 15, 2013 (referred to as the "Customer Class").

3. As a result of Defendants' failures, the Customer Class was victimized by cybercriminals who exploited Defendants' lax security and obtained Customer Class Members' personal identifying information. As such, Mr. Schafer, on behalf of himself and similarly situated customers, brings this class action to redress the harm caused by Defendants' failures.

4. As a result of Target's actions or inactions, Plaintiffs and the proposed Customer Class are now forced to take remedial steps to protect themselves from future loss. Indeed, all of the Customer Class Members are currently at higher risk of direct monetary theft and/or identity theft. As a result of Target's failures, Customer Class Members require measures to protect themselves from theft such as long term credit monitoring, replacement of credit and debit cards, changing of passwords, and other steps which are reasonable and necessary to prevent and mitigate future loss.

5. Financial institutions located in Wisconsin ("Banking Class") have been harmed by Target's security breach based on the cost of canceling and re-issuing credit and debit cards, monitoring accounts, reimbursing customers for fraudulent charges, incurring administrative expenses and overhead charges, compliance costs associated with credit and debit card disposal, and may incur other related damages in the future. As such, Integrity, on behalf it itself and similarly situated financial institutions in Wisconsin, brings this class action to redress the harm caused by Defendants' failures.

PARTIES

6. Plaintiff Kas Schafer is an individual who resides in this Judicial District. Mr. Schafer is a Target customer who purchased items at a Target retail store located in the Western District of Wisconsin between November 27, 2013 and December 15, 2013. Mr. Schafer was advised by his bank that Target had contacted the bank to notify the bank that Mr. Schafer's debit card and accompanying personal identifying information had been compromised in the security breach. As of the present time Mr. Schafer has not received any personal notification of the security breach from Target directly. Mr. Schafer was forced to immediately withdraw money from his account to live on for weeks while his debit card was canceled and while he waited for a replacement card. He will require long term credit and/or identity theft monitoring services.

7. Plaintiff Integrity First Bank ("Integrity") is a Wisconsin bank headquartered at 101 Grand Avenue, Wausau, WI. Integrity cancelled and re-issued credit and debit cards to many of its customers who had made purchases from Target during the relevant time frame. Integrity has suffered and will suffer monetary harm by virtue of canceling and re-issuing cards, monitoring accounts, reimbursing customers for fraudulent charges, incurring administrative expenses and overhead charges, all as a result of Target's failure to reasonably protect its customers' personal identifying information.

8. Defendant Target Corporation is headquartered at 1000 Nicollet Mall, Minneapolis, MN 55403. Target operates general merchandise stores in the United States. Further, Target Corporation provides general merchandise through its website, target.com, and a branded proprietary Target Debit Card. Target Corporation is licensed to do and is doing business in this judicial district.

9. Defendant Target.com is a Minnesota corporation headquartered at 1000 Nicollet Mall, Minneapolis, MN 55403and is an e-commerce site as part of Target Corporation's discount retail corporation. Upon information and belief Target Corporation does business on-line under the name of Target.com, and is doing business in this Judicial District.

JURISDICTION AND VENUE

10. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332 (d)(2). In the aggregate, Plaintiff's claims and the claims of the other members of the Class exceed $5,000,000 exclusive of interest and costs, and there are numerous Class Members who are citizens of states other than Defendants' state of citizenship, which is Minnesota.

11. This Court has personal jurisdiction over Defendants because Defendants are authorized to do business in the State of Wisconsin and in fact do conduct business within the State of Wisconsin, and operate stores within this Judicial District.

12. Venue is proper in this Court pursuant to 28 U.S.C § 1391 because many of the actions and transactions that give rise to this action occurred in the District and because Defendants are subject to personal jurisdiction in this District.

GENERAL ALLEGATIONS

13. Identity theft, which costs Americans tens of billions of dollars per year, occurs when an individual's personal identifying information is used without his or her permission to commit fraud or other crimes.

14. According to the Federal Trade Commission ("FTC"):

> Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

15. The information Defendants lost, including Plaintiffs' identifying information and other financial information, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC"). FTC, About Identity Theft, available at <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/aboutidentity-theft.html> (visited March 23, 2011). Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes. *Id.* The FTC estimates that as many as 9 million Americans have their identities stolen each year. *Id.*

16. Identity thieves can use identifying data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, and/or credit cards. *Id.*

17. The Government Accounting Office ("GAO") has stated that identity thieves can use identifying data to open financial accounts and incur charges and credit in a person's name. As the GAO has stated, this type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim's credit rating. Like the FTC, the GAO has explained that victims of identity theft face

"substantial costs and inconvenience repairing damage to their credit records," as well as the damage to their "good name."

18. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2008: In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, ... individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non- financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration. In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors. The President's Identity Theft Task Force Report at p.21 (Oct. 21, 2008), available at <http://www.idtheft.gov/reports/StrategicPlan.pdf>.

19. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches: [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. GAO, Report to Congressional Requesters, at p.33 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf>.

20. Identity theft crimes often encompass more than just immediate financial loss. Identity thieves often hold onto stolen personal and financial information for several years before using and/or selling the information to other identity thieves.

21. Target has recognized that debit card and credit care information is highly sensitive and must be protected. According to Target's December 11, 2013, Privacy Policy, "[B]y interacting with Target, [customers] consent to use of information that is collected or submitted as described in this privacy policy." Target states:

> We maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information.

22. Many private industries, such as the Payment Card Industry Security Standards Council, set forth detailed security protocols for businesses that obtain personally identifying information for their customer. Unfortunately, upon information and belief, Target is in violation of the Payment Card Industry Security Standard, and numerous other basic standards, because of the following conduct:

(1) improperly storing and retaining credit card transaction and customer data in an unsecured and unauthorized manner;

(2) failing to take all reasonable steps to destroy, or arrange for the destruction of customer records within its custody or control containing personal information which is no longer authorized to be retained by the business by failing to erase or otherwise modify the personal information to make such unreadable or undecipherable through any means;

(3) failing to properly install, implement, and maintain an adequate firewall to protect consumer data;

(4) failing to properly analyze and restrict IP addresses to and from its computer systems and servers;

(5) failing to perform dynamic packet filtering;

(6) failing to properly restrict access to its computers;

(7) failing to properly protect stored data;

(8) failing to adequately encrypt cardholder data and other sensitive information;

(9) failing to properly implement and update adequate anti-virus and anti- spyware software that would properly prevent unauthorized data transmissions caused by viruses, executables or scripts from its servers or computer systems;

(10) failing to track and monitor all access to network resources and cardholder data; and

(11) failing to regularly test security systems and processes or maintain an adequate policy that addresses information security, or to run vulnerability scans.

23. Upon information and belief, at the time of the breach, Defendants stored its customers' Sensitive Personal Information on its “Target Payment Card Data” system in violation of Payment Card Industry ("PCI") data security standards and/or card association standards and/or statutes and/or regulations aimed at protecting such information.

24. As one PCI forensic investigator noted:

> For a hacker to be able to infiltrate Target’s network and access the POS application, several PCI-DSS and PA-DSS controls must not have been implemented effectively. Thus, Target was not compliant during the time of the breach. . . .

> How can I be so sure? We handle these investigations for the payment card brands, and in all of the investigations we performed, the merchant was not compliant to PCI-DSS controls during a breach.[1]

25. As widely reported by multiple news services on December 19, 2013: "Investigators believe the data was obtained via software installed on machines that customers use to swipe magnetic strips on their cards when paying for merchandise at Target stores." http://www.cbsnews.com/news/target-confirms-massive-credit-debit- carddata-breach/.

26. As this news broke, Target finally released a statement concerning the data breach, but not one designed to notify affected customers directly. Rather, Target posted a statement on its corporate website (not on the shopping site regularly accessed by customers) on December 19, 2013, confirming "that the information involved in this incident included customer name, credit or debit card number, and the card's expiration date and CVV (the three-digit security code)." <https*://I*corporate.target.com/discover/article/Important-Notice-Unauthorized-access- to-payment-ca>.

27. "The type of data stolen- also known as 'track data'- allows crooks to create counterfeit cards by encoding the information onto any card with a magnetic stripe." http://krebsonsecurity.com/.

28. The thieves may also have accessed PIN numbers for affected customers' debit cards, allowing the thieves to withdraw money from those customers' bank accounts. (*Id.*)

29. Thieves could not have accessed this information and installed the software on Target's point-of-sale machines but for Defendants' negligence.

30. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.

31. Upon information and belief, Target new of the Security Breach as early as December 11, 2013.

32. On the morning of Sunday, December 15, 2013, Target's Chairman and CEO personally learned of the Security Breach.

33. On December 19, 2013, Target finally confirmed that it was aware of unauthorized access to payment card data that impacted customers making credit card and debit card purchases in its United States' stores.

34. Target initially attempted to convey to its customers that it had "identified and resolved the issue," it is now clear that such attempts to pacify its customers were premature at best. In fact, it has now been confirmed that the data breach was much more extensive than originally indicated.

---

[1] *See* Ericka Chickowski, *Target Breach Should Spur POS Security, PCI 3.0 Awareness,* DARK READING (Dec. 24, 2013) (quoting Ken Stasiak, CEO of SecureState) (available at: http://www.darkreading.com/risk/target-breach-should-spur-pos-security-p/240164960) (last accessed Jan. 27, 2014.)

35. In a *CNBC* article dated January 11, 2014, entitled "Target data breach: Beyond Cards?," it was noted in pertinent part:

> A revelation by Target showed its holiday data breach spanned far wider than originally expected, raising new questions about exactly how such an expansive hack took place. ***The retailer said Friday that its investigation had uncovered an additional 70 million customers may have had their names, mailing addresses, phone numbers, and email addresses stolen.*** Previously, Target said the breach occurred on the terminals where customers swiped credit and debit cards, compromising certain financial information of 40 million shoppers between Nov. 27 and Dec. 15, 2013.
>
> ***Friday's update, however, raises concern that the wider breach took place elsewhere in Target's customer infrastructure. Target first said the only information affected was stored in the magnetic strips on the back of customers' cards; a week later the retailer admitted customers' encrypted PIN data had also been obtained. But personal information about shoppers – such as names, addresses and telephone numbers - are not stored anywhere on a credit or debit card,*** according to bank and credit card officials interviewed by CNBC.
>
> Rodney Joffe, a cybersecurity expert at data firm Neustar, highlights the possibility that breaches extended beyond the point of sale in Target stores. ***"Given the information gathered, it would appear to be account information taken from internal accounting or marketing systems,"*** Joffe told CNBC. "My guess is that a marketing database was accessed, not necessarily financial."
>
> A Target spokesperson did not respond to a request for comment on whether the breach extended to Target.com or other databases that may store customer information. The spokesperson, Molly Snyder, maintained the breach took place during the previously disclosed two-week period.

36. Thereafter, in an article dated January 13, 2014 in *USA Today*, entitled "Authorities are Taking a Close Look at Who Hacked into Target's Customer Information Database," it was further noted in part:

> As computer experts peel back the layers of Target's massive data breach, federal and state law enforcement agencies are running parallel investigations to find the cyber criminals who infiltrated the retailer's computers.
>
> ***Target reported Friday that the cyber thieves compromised the credit card data and personal information of as many as 110 million customers. That data includes phone numbers, email and***

home addresses, credit and debit card numbers, PINs, expiration dates and magnetic strip information.

"The Secret Service will confirm that it is investigating this incident," spokesman Brian Leary said. "It is an ongoing investigation and we can provide no further comment."

The U.S. Secret Service leads an Electronic Crimes Task Force that brings together federal, state and local law enforcement, prosecutors, computer experts and academics to detect and trace attacks on the nation's financial and computer networks, including identity theft, credit card fraud and bank fraud.

While police hunt for the cyber criminals, attorneys general nationwide say they will look more closely at whether Target provided enough protection for its customers.

"Consumers in New York and around the country expect and deserve companies that protect their personal information when they shop on their websites and in their stores," New York Attorney General Eric Schneiderman said in a statement.

North Carolina Attorney General Roy Cooper said his state would also join the investigation and is seeking information from Target about how many North Carolina consumers may be exposed. ***Criminals with contact information can target consumers with telemarketing scams, identity theft and phishing***, Cooper said.

North Carolina law requires businesses to notify customers and the attorney general if their personal information is compromised.

"Putting millions of people's personal information at risk is unacceptable," Cooper said. "Companies must do a better job of protecting their customers if they want to earn their business and their trust."

37. Days later, Target sent correspondence to some, but not all, of its customers which stated:

Dear Target Guest,

As you may have heard or read, Target learned in mid-December that criminals forced their way into our systems and took guest information, including debit and credit card data. ***Late last week, as part of our ongoing investigation, we learned that additional information, including name, mailing address, phone number or email address, was also taken. I am writing to make you aware that your name, mailing address, phone number or email address may have been taken during the intrusion.***

I am truly sorry this incident occurred and sincerely regret any inconvenience it may cause you. Because we value you as a guest and your trust is important to us, ***Target is offering one year of free credit monitoring to all Target guests who shopped in U.S. stores***, through Experian's® ProtectMyID® product which includes identity theft insurance where available. ***To receive your unique activation code for this service, please go to creditmonitoring.target.com and register before April 23, 2014.*** Activation codes must be redeemed by April 30, 2014.

In addition, to guard against possible scams, always be cautious about sharing personal information, such as Social Security numbers, passwords, user IDs and financial account information. Here are some tips that will help protect you:

- Never share information with anyone over the phone, email or text, even if they claim to be someone you know or do business with. Instead, ask for a call-back number.
- Delete texts immediately from numbers or names you don't recognize.
- Be wary of emails that ask for money or send you to suspicious websites. Don't click links within emails you don't recognize. Target's email communication regarding this incident will never ask you to provide personal or sensitive information.

Thank you for your patience and loyalty to Target. You can find additional information and FAQs about this incident at our Target.com/databreach website.

If you have further questions, you may call us at 866-852-8680.

Gregg Steinhafel

Chairman, President and CEO

38. In addition, in a nationally broadcast interview, Target's CEO advised concerned customers to cancel their debit or credit cards and get new cards, placing an additional burden on the Banking Class.

39. When Target customers in the Individual Class follow the CEO's advice and replace their credit and debit cards, the Banking Class is exposed to an additional burden of compliance with § 134.97 Wis. Stat., in addition to the actual cost of cancellation and replacement of the cards.

40. Target has offered little more than a short term "fix" in the way of "credit monitoring" even though identity theft may occur for years after such a massive data breach.

Moreover, Target is requesting that its customers visit its website to apply for an "activation code" concerning such credit monitoring when there is no evidence that Target's systems are safe or that consumers have received this email with the letter contained within from a legitimate source. In addition, not all victims of the breach even received the letter.

41. On January 17, 2014, an article entitled "The Target Data Breach is Becoming a Nightmare" was issued by *Forbes.* That article addresses the above letter distributed by Target and notes in pertinent part:

> Over the past month, details about the breadth of the Target [TGT -1.73%] data breach have continued to emerge. It's not a pretty story. Bad enough when it appeared that through some means, hackers had gotten data all the way from credit card swipe machines out the other side of Target's systems, including encrypted Pin numbers from debit cards. Then it was announced that other information was also stolen, specifically name, address, phone number and/or email address. I assumed this was all somehow related to the same attack. Perhaps a different database, but all information gathered from those who shopped from mid-November through mid-December 2013. Then last night (like colleague Claire O'Connor), I received *my* copy of "the letter."
>
> ***In case you haven't received one, I found a copy of the letter online at marketplace.org. It's identical to the one I received. This is a very significant letter, especially addressed to someone like me, since I haven't shopped at Target stores in recent memory, and possibly shopped at Target.com over a year ago. In other words, the data captured was far broader than we originally imagined. This is bad.***
>
> Other details emerged Thursday about how the breach occurred. Until then everyone, including me, speculated wildly about how this could have been done. And we focused on one point of attack – the POS system. There are standards retailers follow, set forth by the payment industry (led by Visa V -0.11%) that are meant to keep data safe. But it turns out that if a bad guy can break into the corporate system itself, all those standards are pretty useless. And that's what happened. If you're feeling particularly geeky, you can read an excellent explanation of the attack here, at www.krebsonsecurity.com. I'll try to give a simpler overview for the rest of us. The software used to hack the POS system is a variant on one that is commercially available on Cybercrime forums (note: Seriously??? Cybercrime forums? And our governments allow those forums to continue?), for the robust sum of $1,800 for the "budget version" and $2,300 for the "full version," which also allows the bad guys to encrypt the data they've stolen.

This is bad enough, but the real question remains – "How did they gain access to Target's systems?" And they didn't gain access just once. In fact, they kept coming back to harvest data almost daily over the course of several weeks. As we now know, they didn't just stop with the sales data. They roamed across Target's network of servers looking for interesting information, like email addresses, etc. The answer is apparently found in what is known as "Port 80." Let me try to give you a layman's explanation of this.

We have software firewalls on our personal computers (if you don't, you really should). This is the software that warns you if you're being directed to a malicious web site. It also insures you don't get malware planted on your computer if you somehow find yourself on one of those, or get an email with that type of software in it. Large enterprises have both hardware and software firewalls designed to do essentially the same thing, just on a more robust scale. The software and hardware essentially seal up all ways in and out of your computer – except for a very few exceptions. One of those exceptions is the route (or "Port") used for internet browsing traffic. You can't close it – not if you want to use the internet. So we rely on software to separate bad apples from the good ones. ***Long story short, the hackers convinced Target firewalls that they were "good guys." And once they'd done that, they continued to roam freely around Target's system. They've found data old and new and will use it the way they choose.***

Personally, there's not too much they can do with whatever data they got from me. I haven't shopped at Target in a long time, and they have no credit card number info on file. ***But imagine if they grabbed not just your credit card swipe information, but were able to match it up with the other information: address and phone number info as well. They could do a LOT of damage. And that probably explains why finally, banks like Citibank announced they were reissuing all debit cards that were possibly involved in the breach. It's no longer adequate to just change the Pin numbers. Now, it's a do-over.*** I think this was a wise move. As I've mentioned before, I'm frankly pretty befuddled that the entire ecosystem did not move faster to replace cards, change Pin numbers…whatever it took to keep us all safe.

And that brings me to the last point, one that is worth consideration. Retail industry watcher and former National Retail Federation CIO Cathy Hotka points out that most industries have cooperative security groups, called ISACs (Information Sharing and Analysis Centers). If you look at web site www.isacouncil.org, you'll find many industries participate this way. When something

> bad happens, they share information. ***Retailers, for some reason, have chosen not to create this type of group despite potential assistance from USCERT, the FBI and other enterprises.*** Cathy (and now I) expresses real befuddlement over this gap. There's plenty of precedent. Retailers routinely work together on loss prevention tools and techniques, and lobby hard for more assistance from law enforcement against Organized Retail Crime (ORC). It seems that it's long overdue for the industry to do the same when it comes to Cyber-security.
>
> I can appreciate why retailers wish this issue would just go away. After all, they've each spent a small fortune on Visa's PCI compliance initiatives. It's a hard pill to swallow that a static standard is inadequate in an ever-changing world. And now, there's a belief that moving to a new technology that will replace today's magnetic stripes, called EMV, will solve any remaining problems. The Target breach highlights that there will be no magic bullet. The bad guys will continue to evolve. We must do the same.
>
> ***Consumers have grown weary of privacy invasions. This more than anything, explains the surprisingly vocal reaction to the Target breach vs. the TJ Maxx data breach some years ago.*** Retailers are in for challenging times again. It would be best to see us working together to stay a step ahead of the bad guys.

42. The security breach allowed unauthorized access to confidential consumer information which included at the very least (1) phone numbers, (2) email addresses, (3) home addresses, (4) credit and debit card numbers, (5) PIN numbers, (6) expiration dates, and (7) and magnetic strip information, because Target apparently failed to take proper security precautions, and ignored guidelines from government agencies and basic security protocols.

43. Target was inadequately prepared to address the security breach and did not have the proper policies and procedures in place to respond to customers' concerns. In fact, Target advised upset customers to contact their banks because Target did not have sufficient resources in place to handle the volume of customers with questions and complaints. This placed an additional burden on the Banking Class and required an expenditure of resources because of Target's negligence.

44. As a result of Target's failure to properly secure the Company's servers and safeguard Plaintiffs' and Class Members' personal identifying information, Plaintiffs and Class Members' privacy has been invaded. In addition, all of this personal identifying information can easily be used to steal directly from Class Members or to steal Class Members' identities.

45. As a direct and proximate result of Target's data breach, criminals now have Plaintiffs' and Class Members' personal identifying information, along with the knowledge that Plaintiffs and Class Members are accustomed to receiving emails from Target. Additionally, the data breach makes Plaintiffs and Class Members much more likely to respond to requests from Target or law enforcement agencies for more personal information, such as bank account

numbers, login information or even Social Security numbers. Because criminals know this and are capable of posing as Target or law enforcement agencies, consumers like Plaintiffs and their fellow Class Members are more likely to unknowingly give away their sensitive personal information to other criminals.

46. Hence, Target's wrongful actions and inaction in this instance directly and proximately caused the data breach at issue which resulted in the disclosure of Plaintiffs' and Class Members' personal identifying information without their knowledge, authorization and/or consent. As a further direct and proximate result of Target's wrongful actions and/or inaction, Plaintiffs and Class Members have suffered, and will continue to suffer, damages including, without limitation, loss of the unencumbered use of their current passwords, the loss of their passwords, out-of-pocket expenses, loss of privacy, and other economic and noneconomic harm.

47. Plaintiffs and Class Members are now required to monitor their accounts and to respond to identity theft. In order to try to mitigate the damage caused by Defendant, Class Members are also required to take the time to change the passwords on their Target account and may also be required to change passwords on any other website where Plaintiffs and Class Members use the same or a similar password, and change other elements of their compromised personal identifying information. Even taking all of these precautions, Plaintiffs and Class Members still face a very high risk of identity theft.

48. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff Schafer alleges a class action on behalf of himself and:

> Similarly situated Wisconsin residents who made on-line purchases with credit or debit cards from defendants between November 27, 2013 and December 15, 2013, and of all persons (regardless of the State of residency) who made purchases with credit or debit cards at defendants' stores located within the State of Wisconsin during that time period, and whose private information was stolen or otherwise obtained by an unauthorized individual or individuals from Target's servers or other Target computer systems or databases.

This sub-class is referred to as the "Customer Class."

49. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff Integrity alleges a class action on behalf of itself and:

> Similarly situated financial institutions (including banks, savings banks, savings and loan associations or credit unions) located in Wisconsin and authorized to do business in Wisconsin, who have suffered harm as a result of Target's failure to failure to reasonably protect its customers' personal identifying information.

This sub-class is referred to as the "Banking Class."

50. The subclasses are referred to collectively at times in this Complaint as "the Class" or "the Classes". Excluded from both sub-classes are Defendants, their respective officers, directors, and employees, and any entity that has a controlling interest in Defendant, legal representatives, as well as any judge or judicial officer presiding over this case.

51. Plaintiff reserves the right to amend these Class definitions as necessary, including but not limited to, expanding the inclusive dates of the security breach and creation of additional sub-classes.

52. The putative Classes are likely comprised tens of thousands of persons, and hundreds of financial institutions, making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

53. The rights of each sub-Class Member were violated in an identical manner as a result of Defendant's negligent actions and/or inaction.

54. Plaintiffs' claims are typical of the members of the respective sub-Classes, and Plaintiffs can fairly and adequately represent the interests of their respective sub-Class.

55. This action satisfies the requirements of Federal Rule of Civil Procedure 23(b)(2) because Defendants have acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

56. This action satisfies the requirements of Federal Rule of Civil Procedure 23(b)(3) because it involves questions of law and fact common to the members of the respective sub-Classes that predominate over any questions affecting only individual members.

57. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including:

a) Whether Defendant owed a duty to Customer Plaintiffs to exercise reasonable care in protecting and securing their personal identifying information;

b) Whether Defendants unlawfully used, maintained, lost or disclosed Customer Class members' personal and/or financial information;

c) Whether Defendants' conduct was negligent;

d) Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach;

e) Whether the unauthorized disclosure of personal identifying information constitutes an invasion of privacy with respect to the Plaintiff and Class Members;

f) Whether Defendants breached a fiduciary duty owed to Customer Class Members;

g) Whether Plaintiffs and Class Members have been harmed as a result of Defendants' failure to secure and protect their customers' personal identifying information; and

58. The prosecution of separate actions by individual members of the sub-Classes would create a risk of inconsistent or varying adjudications with respect to individual members of each sub-Class, which would establish incompatible standards of conduct for Defendants and would lead to repetitive adjudication of common questions of law and fact. Accordingly, class treatment is superior to any other method for adjudicating the controversy.

59. There are no manageability problems that preclude the maintenance of this case as a class action under Rule 23 (b)(3).

60. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

61. Defendants have acted or refused to act on grounds that apply generally to the class, as alleged above, and certification is proper under Rule 23(b)(2).

FIRST CAUSE OF ACTION -- NEGLIGENCE

62. Plaintiff incorporates as if set forth fully herein all previous paragraphs to this Complaint.

63. Defendants came into possession of Plaintiff's and Customer Class Members' Private Information and had a duty to exercise reasonable care in safeguarding and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

64. Defendants had a duty to timely disclose to plaintiff and all Customer Class Members that their Private Information within its possession had been compromised.

65. Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Customer Class Members' Private Information.

66. Defendants, through their actions and/or omissions, breached their duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding said Private Information within Defendants' possession.

67. Defendants, through their actions and/or omissions, breached their duty to timely disclose to the Plaintiff and the Class Members the fact that their Private Information within defendants' possession had been compromised.

68. § 134.98 Wis. Stats. requires defendants to notify each subject of the security breach of the unauthorized acquisition of personal information pertaining to the subject of the personal information, within 45 days after they learned of the acquisition of personal information. Defendants were also required to notify all consumer reporting agencies of the

timing, distribution, and content of the notices sent to the individuals. Defendants' failure to comply with these requirements is evidence of negligence and/or breach of a legal duty.

69. Defendants' negligent and reckless breach of their duties owed to Plaintiff and the Classes caused Plaintiff and Class Members harm.

70. Plaintiffs seek the award of actual damages on behalf of themselves and the Classes.

SECOND CAUSE OF ACTION –
VIOLATION OF RIGHT TO PRIVACY; § 995.50 Wis. Stats.

71. Plaintiff incorporates as if set forth fully herein all previous paragraphs to this Complaint.

72. Defendants violated plaintiff's and the Customer Class Members' right of privacy when their negligent acts caused the disclosure of private information and such disclosure is of a nature highly offensive to a reasonable person, in a place that a reasonable person would consider to be private, and insofar as defendants knew there was no public interest in the disclosure.

73. The information disclosed was not a matter of public record and was intended to remain private.

74. Defendants expressly or implicitly promised Customer Class Members that such information in their possession would remain private and would not be disclosed or breached.

75. Plaintiff and the Customer Class Members are entitled to equitable relief in order to prevent further invasion of privacy, as well as compensatory damages for pecuniary loss or defendants' unjust enrichment, as well as reasonable attorneys' fees.

THIRD CAUSE OF ACTION -- BREACH OF FIDUCIARY DUTY

76. Plaintiff incorporates as if set forth fully herein all previous paragraphs to this Complaint.

77. By virtue of their possession, custody and/or control of the Plaintiff's and Customer Class Members' Sensitive Personal Information, and their duty to properly monitor and safeguard it, the Defendants were (and continue to be) in a fiduciary relationships with the Plaintiff and Class Members. As fiduciaries, the Defendants owed (and continue to owe) to the Plaintiff and Customer Class Members a fiduciary duty to exercise the highest degree of care, loyalty, and honesty.

78. The Defendants breached their fiduciary duties to the Plaintiff and Customer Class Members by improperly and inadequately storing, monitoring and/or safeguarding the Plaintiff's and Customer Class Members' Sensitive Personal Information.

79. The Defendants breached their fiduciary duties to the Plaintiffs and Customer Class Members by their wrongful actions described above. The Defendants committed these breaches with intentional disregard for the rights of the plaintiff and Customer Class Members.

PRAYER FOR RELIEF

WHEREFORE Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and their Counsel to represent the Class;

B. For injunctive relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Customer Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and Class Members;

C. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

D. For compensation for the cost of long term credit monitoring and long term identity theft monitoring and insurance for the Customer Class, the expense and overhead associated with cancellation, disposal, and re-issuing of cards and monitoring of accounts for fraud by the Banking Class, and for any other damages suffered or expenditures incurred;

E. For an order requiring defendants to submit to periodic compliance audits by a third party regarding the security of consumers' personal identifying information its possession, custody and control.

F. For an award of any other compensatory damages not articulated above and punitive damages in an amount to be determined;

G. For an award of reasonable attorneys' fees and costs;

H. Such other and further relief as this court may deem just and proper.

Dated: 02/13/14

By: /s/ ERIC J. HAAG

Atterbury, Kammer & Haag, S.C.
8500 Greenway Blvd., Ste. 103
Middleton, WI 53562
Phone: 608-821-4600
Fax: 608-821-4610
Email: ehaag@wiscinjurylawyers.com
Attorneys for Plaintiff

Dated: 02/13/14

By: /s/ MICHAEL J. MODL

Axley Brynelson, LLP
2 E. Mifflin Street, Ste. 200
Madison WI 53703
Phone: 608.257.5661
Fax: 608.257.5444
Email: mmodl@axley.com
Attorneys for Plaintiff

JS 44 (Rev. 12/12)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

KAS SCHAFER, an individual, on his own behalf and on behalf of all others similarly situated, and INTEGRITY FIRST BANK, on its own behalf and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Dane
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Atterbury, Kammer & Haag, S.C.
8500 Greenway Blvd., Ste. 103
Middleton, WI 53562

DEFENDANTS

TARGET CORPORATION and TARGET.COM

County of Residence of First Listed Defendant Hennepin County
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☒ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☒ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. Sec. 1332(D)(2)

Brief description of cause:
Negligent and unlawful disclosure of customers' personal identifying information

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☐ Yes ☒ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
02/13/2014

SIGNATURE OF ATTORNEY OF RECORD
/s/ ERIC J. HAAG

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

Print Save As... Reset

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. **Origin.** Place an "X" in one of the six boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 12/09) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Kas Schafer, et al.

Plaintiff

v.

Target Corporation, et al.

Defendant

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Target.com
c/o Carol Oxley
8400 Lakeview Parkway, Ste. 200
Pleasant Prairie, WI 53158

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Attorney Eric J. Haag
Atterbury, Kammer & Haag, S.C.
8500 Greenway Blvd., Ste. 103
Middleton, WI 53562

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

.

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset

AO 440 (Rev. 12/09) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Kas Schafer, et al.

Plaintiff

v.

Target Corporation, et al.

Defendant

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Target Corporation
c/o Carol Oxley
8400 Lakeview Parkway, Ste. 200
Pleasant Prairie, WI 53158

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Attorney Eric J. Haag
Atterbury, Kammer & Haag, S.C.
8500 Greenway Blvd., Ste. 103
Middleton, WI 53562

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

.

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset