

Date Made Public	Name	Type	Description
28-Mar-11	The Briar Group LLC	HACK	A series of breaches at Briar Group restaurants dating back to 2009 led the company to pay \$110,000 in civil penalties to the Commonwealth of Massachusetts. Briar Group was fined for failing to protect the payment card data of tens of thousands of consumers. In addition to having poor data protection practices like allowing employees to share computer passwords and failing to secure network wireless connections, Briar Group was determined to have not responded appropriately when customer data was compromised. A lawsuit alleges that hackers installed and used malicious software to obtain customer debit and credit card information from the Briar Group's computers. The malicious software was on the computers from April 2009 to December of 2009 and the company continued to allow the use of credit and debit cards despite being aware that their computer system had been compromised. The Briar Group agreed to comply with Massachusetts data security regulations, comply with the Payment Card Industry Data Security Standards, develop a secure password management system and implement information security measures.
18-Mar-11	Spoiled Rotten Spa	INSD	The Spoiled Rotten Spa owner was arrested and charged with fraudulently using customer credit card information. Additionally, the owner sold gift certificates to her spa after she had been evicted and could no longer honor them.
15-Mar-11	Nation's Giant Hamburgers	CARD	Over 200 cases of identity theft were traced to Nation's Giant Hamburgers in Vacaville, CA. The cause of the breach was said to be a problem with the credit card machines in the store. The time period when customers using credit cards would have been affected was not reported.
10-Mar-11	Se San Diego Hotel	HACK	Malicious software was uploaded to the Hotel's computer system sometime around September of 2010. Customer credit card information was obtained and sold to a group of seven people who used the information to make fraudulent charges primarily in Central Florida.
24-Feb-11	Snow Creek	HACK	It appears that a hacker was able to obtain unencrypted customer credit card information around Friday February 18. Online customers of the ski resort were not affected. Information from electronic card transactions that were performed on-site was exposed.
22-Feb-11	Jack in the Box	INSD	Investigators determined that a Jack in the Box location had been visited by multiple victims of fraudulent credit and debit card charges. Law enforcement visited the store and found a drive-thru employee with a skimmer in his pocket.
7-Feb-11	Marriott Vacation Club International	PHYS	An unknown number of customer payment slips were lost during shipping. Timeshare maintenance fee payment slips were processed by a bank and shipped back to Marriott. The box of slips arrived damaged and had some of the slips missing. Timeshare owners' names, credit card numbers and expiration dates, and addresses were exposed.
18-Jan-11	Michael's Rock Hill Grille	HACK	Michael's appears to be the common thread in a number of credit card fraud cases in the Southeast. It is believed that someone accessed credit card information by using malware on or obtaining passwords for the system on which the information was stored. The group of affected people most likely includes customers who used their card between September 16 and early December. Many of the cases involved Florida residents, but people in Texas, Kentucky, Tennessee, Georgia and Washington were also affected.
5-Jan-11	Taco Bell	INSD	Two Taco Bell employees were paid to use skimming devices at their store or stores. Between 50 and 100 customers had their credit card information obtained. It is likely that the scam lasted several weeks during the second half of 2010. Two of the men who bought information from the Taco Bell employees were arrested and charged after one of them was recorded buying pre-paid cards.
20-Dec-10	Dino's Pizza, M&T Pizza Inc.	INSD	The former owner of the restaurant was sentenced to five years and five months in prison for identity theft and skimming charges. The former owner was found to have used more than 183 credit numbers from patrons and generally added a fraudulent charge of \$15 to \$30 to each credit or debit card.
14-Dec-10	McDonalds, Arc Worldwide, Silverpop Systems Inc.	HACK	Hackers were able to access the information of McDonald's customers. People who signed up for online promotions or newsletter subscriptions may have had their email addresses, contact information and birth dates exposed. McDonald's uses a company called Arc Worldwide for its marketing services. The breach was through Arc Worldwide's business partner Silverpop Systems Inc.
10-Dec-10	Chicken Express	INSD	An employee brought a skimming device to work and swiped customer debit or credit cards at the drive-thru window. The information was then sold to others who used it to make hundreds of fraudulent bank and gift cards. Authorities became aware of the situation in the summer of 2010. Five hundred customers in Tyler were affected, but customers in other areas were also affected.

20-Nov-10	Desert Rose Resort	HACK	Some guests and employees were affected by a breach or breaches that occurred between June 2010 and October 2010. Credit and debit card information was stolen and misused. The method that criminals used to access the information was not disclosed.UPDATE (11/30/10): Other hotels owned by Desert's parent company Shell Vacation Resorts may have been affected.UPDATE (12/22/10): A notice on Shell's website states that the breach occurred because of a malicious software infection. It was determined that the management system software program of Shell Vacation properties was infected with the malware.
16-Nov-10	Chili's	HACK	Chili's email club service provider InterMundo Media experienced a server breach. No financial information or Social Security numbers were collected for club membership, but full names, email addresses and dates of birth could have been accessed.
1-Nov-10	Thai Cafe	PHYS	An Indianapolis school noticed that their dumpster was being used by someone else. A box of personal information from the Thai Cafe was found to have been illegally dumped. School officials discovered complete payroll stubs from 2000 inside the box and contacted the restaurant owner. The ex-spouse of the restaurant owner apologized for the illegal dumping and claimed that the disposal was handled by a third party.
2-Oct-10	Romeus Cuban Restaurant	CARD	More than two dozen customers had their credit card numbers stolen by a waiter with a skimming device. Authorities believe the former waiter collected information over several months and sold it to a group of identity thieves operating outside of Florida.
29-Sep-10	Cheesecake Factory, PGA Tour Grill, Outback Steakhd	INSD	Two people have been charged with conspiring to commit bank fraud and aggravated identity theft. They paid servers at multiple restaurants in the Washington D.C. area to use skimming devices to collect customer credit card information. The stolen information was used to fraudulently make purchases.
24-Sep-10	Wilderness Ridge, Hidden Valley Golf	HACK	At least 225 reports of credit and debit card fraud have been linked to a security breach that exposed the information of customers of the two golf courses. The affected systems were shutdown. The time of the security breach is unknown.
22-Sep-10	Hana Japanese Sushi Bar and Grill	HACK	Over 30 cases of credit card fraud were linked to the restaurant. The computer server is believed to have been hacked in February of 2010. It appears that the \$50,000 in fraudulent credit charges originated from a hacker in Romania.
20-Sep-10	Julie's Place	HACK	Around a hundred people reported fraudulent charges to their financial accounts after making purchases at the restaurant. A hacker exploited knowledge of vulnerabilities in the Aloha POS software used by the restaurant and obtained customer information. The restaurant changed and upgraded their computer system.
15-Sep-10	Paul Martin's American Bistro	HACK	Hundreds of customers who used their credit cards at Paul Martin's were put at risk for credit card fraud. Hackers accessed the restaurant's credit-card processing system. Customer credit card information was then sold to other criminals and used to make purchases. According to a police news release, the hack did not involve the external financial services network or any third-party data processing service. It appears that the first customers were affected in March of 2010.
11-Sep-10	Cheesecake Factory	INSD	A waiter used a skimming device to make \$100,000 worth of fraudulent charges to customer credit cards. The waiter committed these crimes in late 2008 and was arrested in September of 2010.
8-Sep-10	HEI Hospitality (HEI Hotels and Resorts)	HACK	A vulnerability was discovered in the information systems of multiple hotels. Customers who used credit cards between March 25 and April 17 of 2010 may have had their credit card information exposed.
1-Sep-10	Jason's Deli	HACK	Hundreds of customers may have been affected after using their credit or debit cards at the restaurant. The computer server was infected with a new virus.
20-Aug-10	Turley's Restaurant	PHYS	The owner of Turley's Restaurant went to recycle old employee files. After seeing that the dumpster was full, the owner then left boxes of intact files from former employees near the dumpster. The files included Social Security numbers, birth dates and phone numbers.
13-Aug-10	Doherty Hotel and Convention Center	HACK	Over 150 credit cards used at the Hotel's restaurant were later fraudulently charged. It is believed that the Hotel's database was illegally accessed.
12-Aug-10	Tino's Greek Cafe	CARD	Thieves collected debit and credit card information from customers of Tino's.

11-Aug-10	Ambrosia Asian Bistro	INSD	A waitress admitted to using a skimming device to collect the credit card information of between 50 and 60 customers.
22-Jul-10	The Loft and Comedy Club	DISC	Names, addresses, phone numbers, and credit card information from customers of The Loft and Comedy Club were discovered through a Google search. Customer data from 2004 to 2008 was posted. The Loft fixed the problem and is working on having the site removed.
10-Jul-10	Village of Big Bend	PORT	A laptop containing payroll information for the village's employees was stolen from the car of the village's payroll provider in Milwaukee. Police have not recovered the laptop. The provider reported the theft and sent letters to employees to inform them their personal information was not secure. The provider recommended that employees contact a credit bureau that would place a 90-day alert on their information to prevent identity theft.
9-Jul-10	Emily Morgan Hotel	PHYS	Identity thieves obtained stacks of credit card receipts from one of the hotel's storage rooms in 2006. Hundreds of thousands of dollars in fraudulent charges were then made in three different states. Investigators first became aware of a large identity theft issue in the area during the beginning of 2009. UPDATE (12/4/2010): The ringleader pleaded guilty to ID theft fraud conspiracy, access device fraud and conspiracy to launder money. Seven other co-conspirators have been identified. UPDATE (4/7/2011): A former hotel worker faces up to 22 years in prison for stealing customer information and using it to go on a shopping spree. In 2006, the former employee used credit card receipts from the Emily Morgan hotel in downtown San Antonio to make fraudulent charges totaling \$300,000. This appears to be the one of the largest cases in Alamo City's history. The accused former employee pleaded guilty to three charges and is scheduled to be sentenced in July.
29-Jun-10	Destination Hotels & Resorts	HACK	Hackers have broken into the payment processing system of Destination Hotels & Resorts, a high-end chain best known for its resort hotels in destinations such as Vail, Colorado; Lake Tahoe, California; and Maui, Hawaii. Destination has uncovered a malicious software program inserted into its credit card processing system from a remote source. Destination Hotels is in the process of notifying victims but will not say how many people have had their credit card numbers stolen. The attackers appear to have hit only point-of-sale processing systems, where credit cards are swiped for purchases. Personal information such as guests' home addresses was not compromised. UPDATE (7/2/10): Around 700 customers were affected nationwide by the hack; including dozens of customers of the Driskill Hotel of Austin, Texas.
5-Jun-10	Marco's Restaurant	HACK	The encrypted Internet connection of a restaurant was breached by hackers outside of the organization. Customer credit and debit card information was lost and fraudulently used.
1-Jun-10	Brew HaHa!	HACK	Outdated and improperly managed software caused customer debit and credit cards to be exposed to fraudulent charges. Between 20 and 30 customers of one bank had fraudulent charges from overseas added to their statements. It is not known how many other customers were affected.
25-May-10	Local Coffee	HACK	Hackers may have gained access to credit and debit card information by exploiting Aloha software weaknesses. After a purchase at Local Coffee, a customer's debit card was canceled. This prompted Local Coffee to temporarily stop using Aloha. Another San Antonio eating establishment, Aldaco, also encountered hacking problems while using Aloha software.
24-May-10	Cheesecake Factory	INSD	Three servers from a Cheesecake Factory restaurant were charged with using skimming devices to make over \$117,000 in fraudulent charges to customer credit card accounts.
21-May-10	Aldaco's Mexican Cuisine	HACK	Aldaco's Mexican Cuisine at Stone Oak had a data security breach. Customers were notified of fraudulent charges; some were from places outside of the U.S. Aldaco urged customers who had used their credit cards at the restaurant to cancel them.
18-May-10	The Vine Tavern and Eatery	PHYS	Personal documents including applicant names, Social Security numbers, and dates of birth were found in a dumpster. Customer checks with banking information and credit card receipts were also found. Reports indicate that thousands of pages of information were located.
15-May-10	Mellow Mushroom	HACK	Customers of the Mellow Mushroom eatery had their credit and debit card information hacked sometime around March 11th. Customers of other merchants have been affected, but a hack of Mellow Mushroom's processor is believed to be the source.

9-Apr-10	Mad Capper Saloon & Eatery	HACK	Police have received about 80 complaints of victims' whose credit cards have been compromised. The police have connected the scam to cards used at the Mad Capper Saloon & Eatery. The owner of the Mad Capper Saloon & Eatery has been cooperating with police, he is frustrated that somehow his 30-year-old business is linked to identity theft. The restaurant's owner, has taken steps to make sure his customers are protected. "We've looked into our credit card processing. We've looked into our software program -- our routers in the building, We've scanned everything -- combed it with a fine tooth comb and we can't find anything off of it, so its frustrating."UPDATE (4/10/10): The number of people affected is now nearing 200.
18-Mar-10	Mary's Pizza Shack	HACK	The Plaza location of Mary's Pizza Shack has been identified as the target of Internet hackers who penetrated the restaurant's computer system with a "logger" virus that captured credit card numbers at the transaction terminal. Only credit card numbers were taken by the virus, Albano emphasized, no personal identification information, such as Social Security numbers or bank account records were exposed, although VISA and MasterCard debit accounts were apparently raided. Trustwave identified and removed the virus doing the damage.
13-Mar-10	California Pizza Kitchen	CARD	A credit card thief and his partner used skimming devices to obtain credit card account information. The thief provided his partner with a skimming device while she worked at a California Pizza Kitchen in Plymouth Meeting, Pa. from 2008 to 2009. Around 26 customer credit cards were fraudulently charged.
6-Mar-10	Westin Bonaventure Hotel & Suites	HACK	Westin Bonaventure Hotel & Suites four restaurants in Lake View Bistro, Lobby Court Bar, Bonavista Lounge and L.A. Prime., along with its valet parking operation, may have been hacked at some time between April and December, disclosing names, credit card numbers and expiration dates printed on customers' debit and credit cards.
28-Feb-10	Wyndham Hotels & Resorts	HACK	International hotel group Wyndham Hotels and Resorts (WHR) has suffered yet another serious data breach after hackers broke into its computer systems, stealing customer names and payment card information.UPDATE (5/18/10): An open letter from Wyndham to its customers: <a href="http://www.wyndhamworldwide.com/customer_care/data-claim.cfm">www.wyndhamworldwide.com/customer_care/data-claim.cfm</a>
17-Feb-10	Dairy Queen	HACK	Hanceville police are cautioning residents to be on guard against a sophisticated debit card wire scam that has leached hundreds of thousands of dollars from customers whose card numbers have been stolen remotely from pay terminals at one or more local businesses. The primary target in the theft so far has been the Dairy Queen restaurant. It's unsure whether this is ultimately involving other businesses. At the Dairy Queen location, somebody has apparently tapped into the internet server and hacked into the debit card system. They are printing the customers' debit card numbers and using them all over California and Georgia.
11-Feb-10	Lawrence Welk Resort	HACK	After its security system was disabled, customer credit and debit card information was exposed. The exposure of the information led to some unauthorized transactions.
2-Feb-10	P.F. Chang's Bistro	STAT	According to notification letters from the company: "Password protected electronic equipment belonging to the Company was stolen" on December 19 of 2009. Some current and former employee information was on the equipment. Employee dates of birth and Social Security numbers may be at risk.UPDATE (8/09/10): Another 3,205 people who are residents of Maryland were affected.
22-Jan-10	Brio Tuscan Grille in Country Club Plaza	CARD	A man used a skimming device to obtain the credit card information of customers while working as a waiter at Brio Tuscan Grille of Kansas City, Missouri.UPDATE (7/26/10): The former employee was sentenced to three years of federal prison time for credit card fraud and mail fraud. He originally gained access to the customer information during July and August of 2008. His fraudulent purchases totaled thousands of dollars.