Identity Fraud: Out of Sight, Not Out of Mind

First Financial Bank
www.first-online.com
Member FDIC

September 2018

REGISTRATION & ACTIVATION

For no-cost IDProtect benefits, simply go to **https://www.securechecking.com** using the Access Code provided by First Financial Bank and follow the step-by-step instructions. Please call our Customer Experience Team at 800-511-0045 for assistance with activation or to learn more about IDProtect.

You've seen the movies, read the stories, and received the sensational scam emails. The bumbling, clownish criminals who seem but one step away from a nomination for the Darwin Awards. Those who despite ill intentions and illicit acts remain likable. Or at least fun to mock.

Set that image in contrast to the reality of the cyber criminal. With access to advanced technology tools and mountains of unsecured data, today's cyber criminal operates largely in secrecy and engages in sophisticated, fraudulent attacks on victims – on their finances and identities.

In 2016, a record 15.4 million Americans fell victim to identity fraud.[1] The rise is due largely to the soaring 40% jump in card-not-present (CNP) fraud.[2] CNP refers to transactions where the customer is not required to physically present the card to the merchant, such as online or over the phone. CNP transactions are highly vulnerable to fraud, even with security in place.

Cyber criminals have recognized this weak link in the transaction process and are exploiting it for fraudulent purposes – whether by stealing card or account information, card "testing" by trying a number of small transactions online to see whether card numbers will work or online skimming. Skimming is when hackers exploit the weakness in a point-of-sale system, use malware to steal data and then sell it.

Experts suggest several factors contributed to the surprising increase in CNP fraud.[2]

- ***Use of EMV cards.*** *EMV (or Chip and PIN) cards have made card-present fraud more difficult and fraudsters have responded by aggressively targeting more susceptible channels. It's simply easier and more lucrative for the bad guys to commit fraud with new technologies from afar than in person.*
- ***Rise in online sales.*** *While the growing number of chip cards and EMV terminals make CNP fraud more attractive for criminals, analysts at Javelin Research & Strategy suggest the key driver for CNP fraud is the exploding volume of e-commerce. Research indicates that 80% of Americans now shop online, creating new opportunities for cyber criminals.*
- ***Increase in mobile services.*** *Criminals go where the money is. With the rising number of mobile banking services and transactions plus the overall increase in mobile usage, there is far greater potential for compromise than ever before.*

Protecting yourself from CNP fraud.

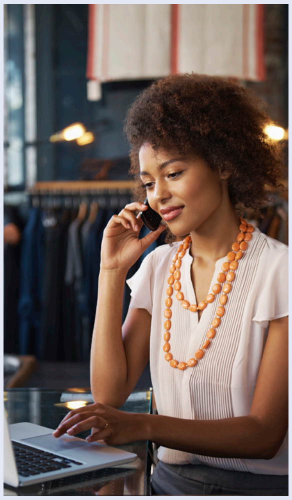
You don't have to suffer the stress of CNP fraud. First Financial Bank suggests several simple steps to help remove the target from your back.

1. Use anti-virus, anti-spyware, and firewall software on your computers, and install updates regularly.
2. Install regular updates to your web browsers and mobile device operating systems.
3. Use strong passwords – that's 8 or more characters with a mix of letters, numbers, and symbols – and change them monthly.
4. Secure your phones by utilizing passcodes, vetting apps before downloading, disabling WiFi when not using and exercising caution when in unsecured WiFi connections.
5. Delete personal, unsecured data from your phone and never email card or bank account numbers.
6. Be wary of emails that appear to be from banks and credit card companies, particularly if they ask for personal information. We'll never do that on email.
7. Before entering personal information online, even with a recognizable retailer, you should find out how the data will be protected, why the company needs it, and with whom it might be shared.
8. Finally, utilize a proven identity protection and monitoring service.

A proven identity theft protection service.

Even the most careful consumer can still fall victim to identity fraud. A comprehensive identity fraud protection service reduces the risk of theft – including CNP fraud – and provides swift, effective resolution in the event of compromise. IDProtect® is included at no additional cost with your First Provider Checking account and provides broad protection for you and your family.[3]

Enjoy proactive identity and credit file monitoring services,[4,5] with monitoring of over 1,000 databases[4] and automated alerts of key changes to your credit report[4]. IDProtect includes access to a 3-in-1 Credit Report every 90 days or upon receipt of a credit alert.[4] And in the unlikely event that fraud occurs, IDProtect provides fully managed theft resolution services, with a detailed recovery plan and up to $10,000 identity theft expense reimbursement coverage[6].



IDPROTECT®
Protection You Can Count On.

[1] Pascual, Al; Marchini, Kyle; Miller, Sarah. 2017 Identity Fraud: Securing the Connected Life. San Francisco: GA Javelin LLC, 2017.
[2] Kitten, T. (2017, February 22). Javelin: Card-Not-Present Fraud Jumped 40% in 2016. Retrieved from http://www.bankinfosecurity.com.
[3] IDProtect service is a personal identity theft protection service available to personal checking account owner(s), their joint account owners and their eligible family members. The service is not available to a "signer" on the account who is not an account owner or to businesses, clubs, trusts, organizations and/or churches and their members, or schools and their employees/students. Family includes: Spouse, persons qualifying as domestic partner, and children under 25 years of age and parent(s) of the account holder who are residents of the same household.
[4] Registration and activation required.
[5] Credit file monitoring may take several days to begin following activation.
[6] Special Program Notes: The descriptions herein are summaries only and do not include all terms, conditions, and exclusions of the Benefits described. Please refer to the actual Guide to Benefit and/or insurance documents for complete details of coverage and exclusions.