



2017 Data Breach Fraud Impact Report: Going Undercover and Recovering Data

14 June 2017 By: Al Pascual

In 2016, FIs were more vigilant about notifying their customers of fraud than ever before. That is the result of several contributing factors, not the least of which are new processes and increasing use of better technology. One of the most oft-discussed reasons for FIs increasing alertness, however, is their growing attention to online criminal communities. Whether FIs are interacting with criminals directly through their internal teams or receiving alerts from vendors about potential customer data being traded on underground forums, they are increasingly protecting customers through their use of subterfuge. This report explores this process, the motivation for FIs, and the thorny issues that can occur when FIs go undercover.

Key questions discussed in this report:

- What was the relationship between data breaches and fraud in 2016?
- What kinds of banking information is bought and sold on criminal forums?
- What outcomes come from FIs conducting online surveillance of criminals?
- What circumstances exist that would cause companies, or their vendors, to exchange payment for that data?
- What legal and ethical concerns that exist when performing such operations?

Consumer data in this report is based on information collected in a random-sample panel survey:

- November 2016 survey of 5,028 consumers. For questions answered by all 5,028 respondents, the maximum margin of sampling error is +/- 1.40 percentage points at the 95% confidence level.

Javelin also conducted a series of interviews involving industry executives and other relevant stakeholders to gain an understanding into the process of obtaining and using breached data. Interviewees represented a variety of organizations, including financial institutions, state and federal law enforcement agencies, and security vendors.

Copyright ©2020 Escalent and/or its affiliates. All rights reserved. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the permission of Escalent.