MAY/JUNE 2019 | FMSinc.org

forward

A PUBLICATION OF THE FINANCIAL MANAGERS SOCIETY

FEATURE

HOSTILE TAKEOVER

Instances of identity fraud and account takeover losses are reaching new peaks. As scammers and fraudsters turn to new methods, how can financial institutions recognize the patterns and protect their customers? We checked in with Andrew Davies, VP of financial crime risk management at Fiserv, to get a better handle on the problem – and what can be done to combat it.

BY THE NUMBERS

16 million
victims of identity fraud in the U.S. in 2017 – an increase of almost 1 million from 2016

120 %
rise in account takeover losses from 2016, as instances of account takeover tripled and total losses from account takeover reached $5.1 billion

16.8 billion
in fraud losses in the U.S. in 2017

1.5 million
victims had an account fraudulently opened in their name – an increase of 200%

The number of social security numbers stolen has overtaken the number of credit card numbers stolen

Source: 2018 Identity Fraud Study, Javelin Strategy and Research

THREE FACTORS DRIVING FRAUD

WHILE HIGH-LEVEL DATA BREACHES LIKE THE EQUIFAX HACK DRAW THE HEADLINES, MORE SUBTLE MACRO FACTORS ARE DRIVING THE SHIFT IN FRAUDSTERS' METHODS.

> "It's called the balloon effect: when you squeeze the balloon in one area, it just pops out somewhere else. Over the last few years, with the introduction of digital chips, cards became more secure, and fraudsters moved to different channels."

1 THE TREND TOWARD DIGITAL INTERACTIONS

The upward trend in account takeover fraud is driven largely by customer demand for digital services. As interactions between financial service providers and their customers move online, fraudsters are capitalizing on the new system much in way scammers of the past used to write hot checks. "In the insurance industry, for example, customers historically purchased insurance products through agents," Davies says. "Now, almost all of these companies have gone direct to consumer through the digital channel – a macro-level trend that drives the way that criminals capture and steal credentials."

2 THE BALLOON EFFECT

Not only do criminals adapt to new ways of doing business, they also know when to ditch scams that have become too difficult. For instance, one of the reasons scammers have moved on to new methods of account fraud is because EMV technology has made debit and credit cards more secure. Davies calls this the balloon effect: "When you squeeze the balloon on one side, it just pops out somewhere else. Over the last few years, with the introduction of digital chips, cards became more secure, and fraudsters simply moved on to different channels."

3 THE TRANSFORMATION OF PAYMENTS

As customers enjoy unprecedented speed and convenience with the latest P2P technologies, the same payment services offer new weaknesses for fraudsters to exploit. "As Charles Dickens famously said in A Tale of Two Cities, 'It was the best of times, it was the worst of times'," Davies explains. "It's the best of times for consumers because you can establish relationships instantaneously and have access to financial services quickly, but it's the worst of times because these things give access to financial criminals, who use those same infrastructures to steal credentials and funds."

THREE FRAUD-FOILING STRATEGIES

THERE ARE PLENTY OF HIGH-TECH METHODS FOR FIGHTING FRAUDSTERS, BUT THE BEST BARRIER CAN BE BOILED DOWN TO THESE THREE PRINCIPLES.

EDUCATE CUSTOMERS

1 The best method for guarding against identity theft and account fraud is for each person to protect their own personal information with the best tools and knowledge possible. Teaching customers how to safeguard their own data should be the first step for any institution. "Many banks and credit unions offer this kind of information on their website," Davies says. "The best practice is for everyone to be very protective of their own data." In the wake of the EU's GDPR, Davies says we may see a rising trend towards individual data sovereignty – a system where everyone has complete and total control of their own personal data.

INCORPORATE THREE LAYERS OF PROTECTION

2 Financial institutions should ensure thorough customer data protection on three levels – identification, authentication and monitoring activity. Identification should take place when the relationship is initially established, while authentication is an ongoing process where customers prove their information is correct through various methods, such as using trial deposits. The final layer is the monitoring of new accounts that could have been opened fraudulently. "The initial layer is when someone first comes to your organization, and the final layer takes place over time, when you look at their account activity for anomalies," Davies says.

FIND THE BALANCE BETWEEN CONVENIENCE AND PROTECTION

3 Of course, it's possible to lock down accounts so thoroughly that no fraudster could get through – but organizations would almost certainly face pushback from customers who appreciate safer accounts, but don't necessarily want to spend ten minutes authenticating their credentials for every balance check. "The convenience element is more impactful for Millennials and Generation Z, who are more likely to nimbly move on from institutions," Davies says. "However, close to 50% of people who are subject to fraud change financial institutions anyway, so it is really important to find that balance between innovative, convenient products and security." ▪

"The convenience element is more impactful for Millennials and Generation Z, who are more likely to nimbly move on from institutions. However, close to 50% of people who are subject to fraud change financial institutions anyway, so it's really important to find that balance between innovative convenient products and security."

forward, a publication of the Financial Managers Society
1 North LaSalle Street | Suite 2225 | Chicago, IL 60602-3916

Published for: **Financial Managers Society, Inc.**
FMSinc.org | 800-ASK-4FMS